PP-Module for Bluetooths

Version: 1.0
2021-04-15
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2021-04-15	Initial Release

Contents

1 Introduction

1.1 Overview

The scope of the Bluetooth PP-Module is to describe the security functionality of Bluetooth technology in terms of [CC] and to define functional and assurance requirements for the Bluetooth capability of mobile devices and operating systems. Bluetooth is a communications standard for short-range wireless transmissions. Bluetooth is implemented in many commercial devices as a method for wirelessly connecting devices or accessories. This PP-Module is intended for use with the following Base-PPs:

- Protection Profile for General Purpose Operating Systems, version 4.3
- Mobile Device Fundamentals, version 3.3

These Base-PPs are valid because consumer-grade desktop and mobile devices may both have Bluetooth hardware radios and so both desktop and mobile operating systems have the software/firmware capability to allow products to use them.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.

Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technical Terms

Authentication	Verifying the identity of communicating devices based on their Bluetooth address. Bluetooth does not provide native user authentication.
Authorization	Allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.
BD_ADDR	The Bluetooth device Address, which is used to identify a Bluetooth device.
BR/EDR	Bluetooth basic rate (BR) and enhanced data rate (EDR).
BR/EDR Controller	A term referring to the Bluetooth Radio, Baseband, Link Manager, and HCI layers.
BR/EDR Piconet Physical Channel	A Channel that is divided into time slots in which each slot is related to an RF hop frequency. Consecutive hops normally correspond to different RF hop frequencies and occur at a standard hop rate of 1600 hops per second. These consecutive hops follow a pseudo-random hopping sequence, hopping through a 79 RF channel set, or optionally fewer channels when Adaptive Frequency Hopping (AFH) is in use. BR/EDR/LE Bluetooth basic rate (BR), enhanced data rate (EDR) and low energy (LE).
Bluetooth	A wireless communication link operating in the unlicensed ISM band at 2.4 GHz using a frequency hopping transceiver. It allows real-time AV and data communications between Bluetooth Hosts. The link protocol is based on time slots.
Bluetooth Baseband	The part of the Bluetooth system that specifies or implements the medium access and physical layer procedures to support the exchange of real-time voice, data information streams, and ad hoc networking between Bluetooth devices.
Bluetooth Controller	A generic term referring to a Primary Controller with or without a Secondary Controller.
Bluetooth Device	A device that is capable of short-range wireless communications using the Bluetooth system.
Bluetooth Device Address	A 48 bit address used to identify each Bluetooth device.
Connect (to service)	The establishment of a connection to a service. If not already done, this also includes establishment of a physical link, logical transport, logical link and L2CAP channel.
Connectable device	A BR/EDR device in range that periodically listens on its page scan physical channel and will respond to a page on that channel. An LE device that is advertising using a connectable advertising event.
Connected devices	Two BR/EDR devices and with a physical link between them. Connecting A phase in the communication between devices when a connection between the devices is being established. The connecting phase follows after the link establishment phase is completed.
Connection	An interaction between two peer applications or higher layer protocols mapped onto an L2CAP channel.
Connection establishment	A procedure for creating a connection mapped onto a channel.
Connection event	A series of one or more pairs of interleaving data packets sent between a master and a slave on the same physical channel.

Creation of a secure connection	A procedure of establishing a connection, including authentication and encryption.
Creation of a trusted relationship	A procedure where the remote device is marked as a trusted device. This includes storing a common link key for future authentication, or pairing, when a link key is not available.
Device discovery	A procedure for retrieving the Bluetooth device address, clock, class-of-device field and used page scan mode from discoverable devices.
Discoverable Mode	A Bluetooth device that is performing inquiry scans in BR/EDR or advertising with a discoverable or connectable advertising event with a discoverable flag set in LE.
Discoverable device	A BR/EDR device in range that periodically listens on an inquiry scan physical channel and will respond to an inquiry on that channel. An LE device in range that is advertising with a connectable or scannable advertising event with a discoverable flag set in the advertising data. This device is in the discoverable mode.
Discovery procedure	A Bluetooth device that is carrying out the inquiry procedure in BR/EDR or scanning for advertisers using a discoverable or connectable advertising event with a discoverable flag set in LE.
Host	A logical entity defined as all of the layers below the non-core profiles and above the Host Controller interface (HCI); i.e. Bluetooth Host attached to a Bluetooth Controller may communicate with other Bluetooth Hosts attached to their Controllers as well.
L2CAP Channel	A logical connection on L2CAP level between two devices serving a single application or higher layer protocol.
L2CAP Channel establishment	A procedure for establishing a logical connection on L2CAP level.
LMP authentication	An LMP level procedure for verifying the identity of a remote device.
LMP pairing	A procedure that authenticates two devices and creates a common link key that can be used as a basis for a trusted relationship or a (single) secure connection.
Link	Shorthand for a logical link.
Link establishment	A procedure for establishing the default ACL link and hierarchy of links and channels between devices.
Link key	A secret that is known by two devices and is used to authenticate the link.
Logical Link Control and Adaptation Protocol (L2CAP)	A data link protocol used in the Bluetooth protocol stack.
Logical link	The lowest architectural level used to offer independent data transport services to clients of the Bluetooth system.
Name discovery	A procedure for retrieving the user-friendly name (the Bluetooth device name) of a connectable device.
OBEX Push	A method of Bluetooth one-way file transfer that is initiated by the entity that is providing the file.
PIN	A user-friendly value that can be used to authenticate connections to a device before pairing has taken place.
Paired device	A Bluetooth device for which a link key has been created (either before connection establishment was requested or during connecting phase).
Piconet	A collection of devices occupying a shared physical channel where one of the devices is the Piconet Master and the remaining devices are connected to it.
Piconet Master	The BR/EDR device in a piconet whose Bluetooth Clock and Bluetooth Device Address are used to define the piconet physical channel characteristics.
Piconet Slave	Any BR/EDR device in a piconet that is not the Piconet Master, but is connected to the Piconet Master.
RFCOMM	A transport protocol used in the Bluetooth protocol stack that emulates RS-232 serial port connections.
Trusted	A device that has a fixed relationship with another device and has full access to all services.

Device	
Unknown device	A Bluetooth device for which no information (Bluetooth Device Address, link key or other) is stored.
Untrusted Device	A device that does not have an established relationship with another Bluetooth device, which results in the untrusted device receiving restricted access to services.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) in this PP-Module is a product that implements Bluetooth functionality. This PP-Module describes the extended security functionality of Bluetooth in terms of CC. This PP-Module extends the Protection Profile for General Purpose Operating Systems or Mobile Device Fundamentals. A compliant TOE will meet all mandatory SFRs defined in this PP-Module in addition to the mandatory SFRs of its claimed Base-PP. For each Base-PP, this PP-Module refines several of the Base-PP's SFRs so that they can accommodate the Bluetooth functionality defined by the PP-Module. A compliant TOE will claim all selection-based SFRs from this PP-Module and its Base-PP as needed based on the relevant selections in other requirements being chosen.

Note that [MDF] evaluation activities require certain tests to be performed against all radios present on the device. When the TOE also claims conformance to a PP-Configuration that includes this PP-Module, those tests are executed against the Bluetooth radio as well.

Also note that each Base-PP defines its own requirements for protection of data at rest. When the TOE also claims conformance to a PP-Configuration that includes this PP-Module, any data that is used by the TOE's Bluetooth implementation is expected to be stored using the same protection mechanisms.

1.3.1 TOE Boundary

The Bluetooth implementation is a logical component executing on an end user personal computing or mobile device. As such, the TOE must rely heavily on the TOE's operational environment (host platform, network stack, and operating system) for its execution domain and its proper usage. The TOE will rely on the IT environment to address much of the security functionality related to administrative functions. The physical boundary of the TOE includes the physical device on which it is installed, as this device will contain an internal or external Bluetooth radio that is used as the physical medium for transmitting and receiving data over the Bluetooth logical channel.

1.4 Use Cases

Requirements in this PP-Module are designed to address the security problems in at least the following use cases. These use cases are intentionally very broad, as many specific use cases exist within these larger categories.

[USE CASE 1] General-Purpose Operating System

This use case is for a Bluetooth TOE that is part of a general-purpose operating system. Specifically, the Bluetooth TOE is expected to be part of the operating system itself and not a standalone third-party application that is installed on top of it.

[USE CASE 2] Mobile Device

This use case is for a Bluetooth TOE that is part of a mobile operating system that runs on a mobile device. Specifically, the Bluetooth TOE is expected to be part of the mobile operating system itself and not a standalone third-party application that is acquired from the mobile vendor's application store.

2 Conformance Claims

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-based SFRs, and Optional SFRs (dated May 2017).

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module.

- Mobile Device Fundamentals, version 3.3
- Protection Profile for General Purpose Operating Systems, version 4.3

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 5.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

Package Claim

This PP-Module does not claim conformance to any packages.

3 Security Problem Description

All threats, assumptions, organizational security policies, and/or objectives that apply to this PP-Module are inherited from the Base-PP to which the TOE also conforms. This PP-Module does not add or remove any elements to the security problem definition given in the Base-PP. The SFRs defined in this PP-Module provide additional mechanisms for mitigating the threats already defined in the Base-PPs due to the fact that including a Bluetooth implementation introduces a new external interface to the underlying general-purpose OS or mobile device platform.

3.1 Threats

This PP-Module defines no additional threats beyond those defined in the base PPs. Note however that the SFRs defined in this PP-Module will assist in the mitigation of the following threats defined in the base PPs:

T.NETWORK_EAVESDROP
: See MDF PP, Section 3.1 and GPOS PP, Section 3.1.

T.NETWORK_ATTACK
: See MDF PP, Section 3.1 and GPOS PP, Section 3.1.

3.2 Assumptions

This document does not define any additional assumptions.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

This PP-Module defines no additional TOE security objectives beyond those defined in the base PPs. Note however that the SFRs defined in this PP-Module will assist in the achievement of the following objectives defined in the base PP:

O.PROTECTED_COMMS
See MDF PP, Section 4.1 and GPOS PP, Section 4.1.

4.2 Security Objectives for the Operational Environment

No environmental security objectives have been identified that are specific to Bluetooth technology. However, any environmental security objectives defined in the Base-PPs will also apply to the portion of the TOE that implements Bluetooth.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.NETWORK_EAVESDROP	O.PROTECTED_COMMS	The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS as this provides the capability to communicate using Bluetooth as a means to maintain the confidentiality of data that are transmitted outside of the TOE.
T.NETWORK_ATTACK	O.PROTECTED_COMMS	The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS as this provides the capability to communicate using Bluetooth as a means to maintain the confidentiality of data that are transmitted outside of the TOE.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Bluetooths PP Security Functional Requirements Direction

In a PP-Configuration that includes the Bluetooths PP, the TOE is expected to rely on some of the security functions implemented by the Bluetooth as a whole and evaluated against the Bluetooths PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the Bluetooths PP in addition to what is mandated by Section 5.3 TOE Security Functional Requirements.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the Bluetooths PP and relevant to the secure operation of the TOE.

5.1.1.1 Security Management (FMT)

FMT_SMF_EXT.1 Specification of Management Functions

FMT_SMF_EXT.1.1

This PP-Module does not modify this SFR as it is defined in the MDF PP. However, note that this PP-Module requires the list of radios specified in the assignment for management function 4 ("enable/disable [**assignment:** *list of all radios*]") to include Bluetooth radios. Bluetooth BR/EDR and Bluetooth LE will be listed separately if the TSF provides the ability to enable/disable them separately (i.e., if management function BT-3 below is claimed). Otherwise, both interfaces will be treated as one radio for that assignment.

Evaluation Activities

FMT_SMF_EXT.1
There is no change to the Base PP EAs for this SFR when this PP-Module is claimed.

5.1.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the Bluetooths PP is claimed as the Base-PP.

5.1.2.1 Security Management (FMT)

FMT_SMF_EXT.1/BT Specification of Management Functions

FMT_SMF_EXT.1.1/BT

The TSF shall be capable of performing the following **Bluetooth** management functions:

#	Management Function	Impl.	User Only	Admin	Admin Only
BT-1	Configure the Bluetooth trusted channel. • Disable/enable the Discoverable (for BR/EDR) and Advertising (for LE) modes;	M	O	O	O
BT-2	Change the Bluetooth device name (separately for BR/EDR and LE);	O	O	O	O
BT-3	Provide separate controls for turning the BR/EDR and LE radios on and off;	O	O	O	O

BT-4	Allow/disallow the following additional wireless technologies to be used with Bluetooth: [**selection**: *Wi-Fi, NFC, [**assignment**: other wireless technologies]*];	O	O	O	O
BT-5	Configure allowable methods of Out of Band pairing (for BR/EDR and LE);	O	O	O	O
BT-6	Disable/enable the Discoverable (for BR/EDR) and Advertising (for LE) modes separately;	O	O	O	O
BT-7	Disable/enable the Connectable mode (for BR/EDR and LE);	O	O	O	O
BT-8	Disable/enable the Bluetooth [**assignment**: *list of Bluetooth service and/or profiles available on the OS (for BR/EDR and LE)*];	O	O	O	O
BT-9	Specify minimum level of security for each pairing (for BR/EDR and LE);	O	O	O	O

Application Note: As is the case with the [MDF PP], the first column lists the management function, the second column lists whether it is mandatory to implement the function and the remaining columns indicate whether it is mandatory, optional, or prohibited to implement the function by role as follows:

- The third column indicates functions that are to be restricted to the user (i.e. not available to the administrator).
- The fourth column indicates functions that are available to the administrator. These functions can still be available to the user, as long as the function is not restricted to the administrator (column 5).
- The fifth column indicates whether the function is to be restricted to the administrator when the device is enrolled and the administrator applies the indicated policy (i.e., MDM administration). This does not prevent the user from modifying a setting to make the function stricter, but the user cannot undo the configuration enforced by the administrator.

For columns 2-5, an 'M' indicates that it is mandatory, an 'O' indicates that it is optional, and a '-' indicates that it is prohibited.

(BT-1.) Management of the Discoverable and Advertising mode and management of the Bluetooth device name are mandatory. All other management functions for Bluetooth are currently objective.

(BT-2. optional) Requires management of the Bluetooth device name separately for BR/EDR and LE radios.

(BT-4. optional) May include disabling Wi-Fi being used as a part of Bluetooth High Speed and/or disabling NFC as an Out of Band pairing method for Bluetooth. May also include other wireless technologies beyond those already specified.

(BT-8. optional) The Bluetooth services and/or profiles that may be disabled should be listed for the user or administrator either by service and/or profile name or by the types of applications for which the service and/or profile is used.

(BT-9. optional) The minimum level of security permitted may be configurable for each individual pairing or for all Bluetooth pairings.

- If the TSF supports any of the BR/EDR security modes in the following list; it should provide a mechanism for the user to choose the minimum level of security to enforce for a particular device during the pairing process: Security Mode 1 (any level); Security Mode 2; (any level); Security Mode 3; (any level); Security Mode 4; Levels 0;1;2 (aside from the services permitted to use Mode 4; Level 0 in Bluetooth Core Specification version 4.2; Vol. 3; Part C; p. 325).
- If the TSF supports any of the LE security modes in the following list; it should provide a mechanism for the user to choose the minimum level of security to enforce for a particular device during the pairing process: Security Mode 1: Levels 1, 2; Security Mode 2, (any level).
- Examples of levels of security are the use of legacy pairing; the use of different types of Secure Simple Pairing; a requirement for Man-in-the-Middle protection; the enforcement of Secure Connections Only mode; etc.

Function-specific Application Notes:

Management of the Discoverable and Advertising mode and management of the Bluetooth device name are mandatory. All other management functions for

Bluetooth are currently objective.

Function BT-3 requires management of the Bluetooth device name separately for BR/EDR and LE radios.

May include disabling Wi-Fi being used as a part of Bluetooth High Speed and/or disabling NFC as an Out of Band pairing method for Bluetooth. May also include other wireless technologies beyond those already specified.

The Bluetooth services and/or profiles that may be disabled should be listed for the user or administrator either by service and/or profile name or by the types of applications for which the service and/or profile is used.

The minimum level of security permitted may be configurable for each individual pairing or for all Bluetooth pairings.

- If the TSF supports any of the BR/EDR security modes in the following list; it should provide a mechanism for the user to choose the minimum level of security to enforce for a particular device during the pairing process: Security Mode 1 (any level); Security Mode 2; (any level); Security Mode 3; (any level); Security Mode 4; Levels 0;1;2 (aside from the services permitted to use Mode 4; Level 0 in Bluetooth Core Specification version 4.2; Vol. 3; Part C; p. 325).
- If the TSF supports any of the LE security modes in the following list; it should provide a mechanism for the user to choose the minimum level of security to enforce for a particular device during the pairing process: Security Mode 1: Levels 1, 2; Security Mode 2, (any level).
- Examples of levels of security are the use of legacy pairing; the use of different types of Secure Simple Pairing; a requirement for Man-in-the-Middle protection; the enforcement of Secure Connections Only mode; etc.

Evaluation Activities

FMT_SMF_EXT.1/BT
TSS
The evaluator shall ensure that the TSS includes a description of the Bluetooth profiles and services supported and the Bluetooth security modes and levels supported by the TOE.

Guidance
The evaluator shall ensure that the management functions defined in the PP-Module are described in the guidance to the same extent required for the Base-PP management functions.

Tests
The evaluator shall use a Bluetooth-specific protocol analyzer to perform the following tests:

The following EAs correspond to specific management functions.
Function BT-1
Tests
For , the evaluator shall disable the Discoverable mode and shall verify that other Bluetooth BR/EDR devices cannot detect the TOE. The evaluator shall use the protocol analyzer to verify that the TOE does not respond to inquiries from other devices searching for Bluetooth devices. The evaluator shall enable Discoverable mode and verify that other devices can detect the TOE and that the TOE sends response packets to inquiries from searching devices.

Function BT-2 [CONDITIONAL]
Tests
The evaluator shall examine Bluetooth traffic from the TOE to determine the current Bluetooth device name, change the Bluetooth device name, and verify that the Bluetooth traffic from the TOE lists the new name. The evaluator shall examine Bluetooth traffic from the TOE to determine the current Bluetooth device name for BR/EDR and LE. The evaluator shall change the Bluetooth device name for LE independently of the device name for BR/EDR. The evaluator shall verify that the Bluetooth traffic from the TOE lists the new name.

Function BT-3 [CONDITIONAL]
Tests
The evaluator shall disable Bluetooth BR/EDR and enable Bluetooth LE. The evaluator shall examine Bluetooth traffic from the TOE to confirm that only Bluetooth LE traffic is present. The evaluator shall repeat the test with Bluetooth BR/EDR enabled and Bluetooth LE disabled, confirming that only Bluetooth BR/EDR is present.

Function BT-4 [CONDITIONAL]
TSS
If function BT-4, "Allow/disallow additional wireless technologies to be used with Bluetooth," is selected, the evaluator shall verify that the TSS describes any additional wireless technologies that may be used with Bluetooth, which may include Wi-Fi with Bluetooth High Speed and/or NFC as an Out of Band pairing mechanism.

Tests
(conditional): For each additional wireless technology that can be used with Bluetooth as

claimed in the ST, the evaluator shall revoke Bluetooth permissions from that technology. If the set of supported wireless technologies includes Wi-Fi, the evaluator shall verify that Bluetooth High Speed is not able to send Bluetooth traffic over Wi-Fi when disabled. If the set of supported wireless technologies includes NFC, the evaluator shall verify that NFC cannot be used for pairing when disabled. For any other supported wireless technology, the evaluator shall verify that it cannot be used with Bluetooth in the specified manner when disabled. The evaluator shall then re-enable all supported wireless technologies and verify that all functionality that was previously unavailable has been restored.

Function BT-5 [CONDITIONAL]
TSS
If function BT-5, "Configure allowable methods of Out of Band pairing (for BR/EDR and LE)," is selected, the evaluator shall verify that the TSS describes when Out of Band pairing methods are allowed and which ones are configurable.

Tests
(conditional): The evaluator shall attempt to pair using each of the Out of Band pairing methods, verify that the pairing method works, iteratively disable each pairing method, and verify that the pairing method fails.

Function BT-6 [CONDITIONAL]
TSS
If function BT-8, "Disable/enable the Bluetooth services and/or profiles available on the OS (for BR/EDR and LE)," is selected, the evaluator shall verify that all supported Bluetooth services are listed in the TSS as manageable and, if the TOE allows disabling by application rather than by service name, that a list of services for each application is also listed.

Tests
(conditional): The evaluator shall enable Advertising for Bluetooth LE, verify that the advertisements are captured by the protocol analyzer, disable Advertising, and verify that no advertisements from the device are captured by the protocol analyzer.

Function BT-7 [CONDITIONAL]
Tests
The evaluator shall enable Connectable mode and verify that other Bluetooth devices may pair with the TOE and (if the devices were bonded) re-connect after pairing and disconnection. For BR/EDR devices: The evaluator shall use the protocol analyzer to verify that the TOE responds to pages from the other devices and permits pairing and re-connection. The evaluator shall disable Connectable mode and verify that the TOE does not respond to pages from remote Bluetooth devices, thereby not permitting pairing or re-connection. For LE: The evaluator shall use the protocol analyzer to verify that the TOE sends connectable advertising events and responds to connection requests. The evaluator shall disable Connectable mode and verify that the TOE stops sending connectable advertising events and stops responding to connection requests from remote Bluetooth devices.

Function BT-8 [CONDITIONAL]
Tests
For each supported Bluetooth service and/or profile listed in the TSS, the evaluator shall verify that the service or profile is manageable. If this is configurable by application rather than by service and/or profile name, the evaluator shall verify that a list of services and/or profiles for each application is also listed.

Function BT-9 [CONDITIONAL]
TSS
If function BT-9, "Specify minimum level of security for each pairing (for BR/EDR and LE)," is selected, the evaluator shall verify that the TSS describes the method by which the level of security for pairings are managed, including whether the setting is performed for each pairing or is a global setting.

Tests
The evaluator shall allow low security modes/levels on the TOE and shall initiate pairing with the TOE from a remote device that allows only something other than Security Mode 4/Level 3 or Security Mode 4/Level 4 (for BR/EDR), or Security Mode 1/Level 3 (for LE). (For example, a remote BR/EDR device may claim Input/Output capability "NoInputNoOutput" and state that man-in-the-middle (MiTM) protection is not required. A remote LE device may not support encryption.) The evaluator shall verify that this pairing attempt succeeds due to the TOE falling back to the low security mode/level. The evaluator shall then remove the pairing of the two devices, prohibit the use of low security modes/levels on the TOE, then attempt the connection again. The evaluator shall verify that the pairing attempt fails. With the low security modes/levels disabled, the evaluator shall initiate pairing from the TOE to a remote device that supports Security Mode 4/Level 3 or Security Mode 4/Level 4 (for BR/EDR) or Security Mode 1/Level 3 (for LE). The evaluator shall verify that this pairing is successful and uses the high security mode/level.

5.2 Bluetooths PP Security Functional Requirements Direction

In a PP-Configuration that includes the Bluetooths PP, the TOE is expected to rely on some of the security functions implemented by the Bluetooth as a whole and evaluated against the Bluetooths PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the Bluetooths PP in addition to what is mandated by Section 5.3 TOE Security Functional Requirements.

5.2.1 Modified SFRs

The SFRs listed in this section are defined in the Bluetooths PP and relevant to the secure operation of the TOE.

5.2.1.1 Security Management (FMT)

FMT_MOF_EXT.1 Management of Security Functions Behavior

FMT_MOF_EXT.1.1

There is no change to the text of this SFR. The SFR references FMT_SMF_EXT.1 and states that the OS shall permit the administrator role to perform the relevant functions listed in FMT_SMF_EXT.1. The function "Enable/Disable the Bluetooth interface" is listed as an optional management function in FMT_SMF_EXT.1 for both users and administrators. When this PP-Module is claimed, the administrator or user role must be able to enable/disable the Bluetooth interface. In other words, the function itself is moved from optional to mandatory, but this PP-Module does not require that it be implemented by a specific role. If the ST indicates that the administrator role can perform this function, then the restrictions imposed by FMT_MOF_EXT.1 will apply to it.

Evaluation Activities

FMT_MOF_EXT.1
There is no change to the Base PP EAs for this SFR when this PP-Module is claimed.

FMT_SMF_EXT.1 Specification of Management Functions

FMT_SMF_EXT.1.1

This PP-Module does not modify this SFR as it is defined in the GPOS PP. However, note that this PP-Module requires the function "Enable/disable Bluetooth interface" to be implemented, though this PP-Module does not mandate whether it be assigned to the Administrator or User role.

Evaluation Activities

FMT_SMF_EXT.1
There is no change to the Base PP EAs for this SFR when this PP-Module is claimed.

5.2.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the Bluetooths PP is claimed as the Base-PP.

5.2.2.1 Security Management (FMT)

FMT_MOF_EXT.1/BT Management of Security Functions Behavior

FMT_MOF_EXT.1.1/BT

The OS shall restrict the ability to perform the function indicated in the "Administrator" column in FMT_SMF_EXT.1.1**/BT** to the administrator.

Application Note: The management functions in FMT_SMF_EXT.1/BT require the function BT-1 to be supported by the TOE and manageable by an Administrator at minimum. All other management functions, and what roles may perform them, are optional. The ST must make it clear which of these functions are provided by the TOE and which roles are able to manage them.

Evaluation Activities

FMT_MOF_EXT.1/BT
TSS
The evaluator shall examine the TSS to ensure that it identifies the Bluetooth-related management functions that are supported by the TOE and the roles that are authorized to perform each function.

Guidance

The evaluator shall examine the operational guidance to ensure that it provides sufficient guidance on each supported Bluetooth management function to describe how the function is performed and any role restrictions on the subjects that are authorized to perform the function.

Tests
For each function that is indicated as restricted to the administrator, the evaluation shall perform the function as an administrator, as specified in the Operational Guidance, and determine that it has the expected effect as outlined by the Operational Guidance and the SFR. The evaluator will then perform the function (or otherwise attempt to access the function) as a non-administrator and observe that they are unable to invoke that functionality.

FMT_SMF_EXT.1/BT Specification of Management Functions

FMT_SMF_EXT.1.1/BT

The OS shall be capable of performing the following **Bluetooth** management functions:

Function	Administrator	User
BT-1. Configure the Bluetooth trusted channel. • Disable/enable the Discoverable (for BR/EDR) and Advertising (for LE) modes;	X	O
BT-2. Change the Bluetooth device name (separately for BR/EDR and LE);	O	O
BT-3. Provide separate controls for turning the BR/EDR and LE radios on and off;	O	O
BT-4. Allow/disallow the following additional wireless technologies to be used with Bluetooth: [**selection**: *Wi-Fi, NFC, [**assignment**: other wireless technologies]*];	O	O
BT-5. Configure allowable methods of Out of Band pairing (for BR/EDR and LE);	O	O
BT-6. Disable/enable the Discoverable (for BR/EDR) and Advertising (for LE) modes separately;	O	O
BT-7. Disable/enable the Connectable mode (for BR/EDR and LE);	O	O
BT-8. Disable/enable the Bluetooth [**assignment**: *list of Bluetooth service and/or profiles available on the OS (for BR/EDR and LE)*];	O	O
BT-9. Specify minimum level of security for each pairing (for BR/EDR and LE);	O	O

Application Note: The ST should indicate which of the optional management functions are implemented in the TOE. This can be done by adjusting the "Administrator" and "User" columns to "X" according to which capabilities are present or not present, and for which privilege level.
(BT-1.) Management of the Discoverable and Advertising mode and management of the Bluetooth device name are mandatory. All other management functions for Bluetooth are currently objective.

(BT-2. optional) Requires management of the Bluetooth device name separately for BR/EDR and LE radios.

(BT-4. optional) May include disabling Wi-Fi being used as a part of Bluetooth High Speed and/or disabling NFC as an Out of Band pairing method for Bluetooth. May also include other wireless technologies beyond those already specified.

(BT-8. optional) The Bluetooth services and/or profiles that may be disabled should be listed for the user or administrator either by service and/or profile name or by the types of applications for which the service and/or profile is used.

(BT-9. optional) The minimum level of security permitted may be configurable for each individual pairing or for all Bluetooth pairings.

- If the TSF supports any of the BR/EDR security modes in the following list; it should provide a mechanism for the user to choose the minimum level of security to enforce for a particular device during the pairing process: Security Mode 1 (any level); Security Mode 2; (any level); Security Mode 3; (any level); Security Mode 4; Levels 0;1;2 (aside from the services permitted to use Mode 4; Level 0 in Bluetooth Core Specification version

4.2; Vol. 3; Part C; p. 325).

- If the TSF supports any of the LE security modes in the following list; it should provide a mechanism for the user to choose the minimum level of security to enforce for a particular device during the pairing process: Security Mode 1: Levels 1, 2; Security Mode 2, (any level).
- Examples of levels of security are the use of legacy pairing; the use of different types of Secure Simple Pairing; a requirement for Man-in-the-Middle protection; the enforcement of Secure Connections Only mode; etc.

Evaluation Activities

FMT_SMF_EXT.1/BT

TSS

The evaluator shall ensure that the TSS includes a description of the Bluetooth profiles and services supported and the Bluetooth security modes and levels supported by the TOE.

If function BT-4, "Allow/disallow additional wireless technologies to be used with Bluetooth," is selected, the evaluator shall verify that the TSS describes any additional wireless technologies that may be used with Bluetooth, which may include Wi-Fi with Bluetooth High Speed and/or NFC as an Out of Band pairing mechanism.

If function BT-5, "Configure allowable methods of Out of Band pairing (for BR/EDR and LE)," is selected, the evaluator shall verify that the TSS describes when Out of Band pairing methods are allowed and which ones are configurable.

If function BT-8, "Disable/enable the Bluetooth services and/or profiles available on the OS (for BR/EDR and LE)," is selected, the evaluator shall verify that all supported Bluetooth services are listed in the TSS as manageable and, if the TOE allows disabling by application rather than by service name, that a list of services for each application is also listed.

If function BT-9, "Specify minimum level of security for each pairing (for BR/EDR and LE)," is selected, the evaluator shall verify that the TSS describes the method by which the level of security for pairings are managed, including whether the setting is performed for each pairing or is a global setting.

Guidance

The evaluator shall ensure that the management functions defined in the PP-Module are described in the guidance to the same extent required for the Base-PP management functions.

Tests

The evaluator shall use a Bluetooth-specific protocol analyzer to perform the following tests:

5.3 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.3.1 Security Audit (FAU)

FAU_GEN.1/BT Audit Data Generation (Bluetooth)

FAU_GEN.1.1/BT

The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions
b. All auditable events for the [*not selected*] level of audit
c. [*Specifically defined auditable events in the Auditable Events table*].

Table 2 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM_EXT.8	None.	
FIA_BLT_EXT.1	Failed user authorization of Bluetooth device.	User authorization decision (e.g., user rejected connection, incorrect pin entry).
	Failed user authorization for local Bluetooth Service.	Bluetooth address and name of device. Bluetooth profile. Identity of local service with [**selection**: *service ID, profile name*].

FIA_BLT_EXT.2	Initiation of Bluetooth connection.	Bluetooth address and name of device.
	Failure of Bluetooth connection.	Reason for failure.
FIA_BLT_EXT.3 (optional)	Duplicate connection attempt.	BD_ADDR of connection attempt.
FIA_BLT_EXT.4	None.	
FIA_BLT_EXT.5 (if claimed)	None.	
FIA_BLT_EXT.6	None.	
FIA_BLT_EXT.7	None.	
FTP_BLT_EXT.1	None.	
FTP_BLT_EXT.2	None.	
FTP_BLT_EXT.3/BR	None.	
FTP_BLT_EXT.3/LE (if claimed)	None.	

FAU_GEN.1.2/BT

The TSF shall record within each audit record at least the following information:

a. Date and time of the event
b. Type of event
c. Subject identity
d. The outcome (success or failure) of the event
e. [*Additional information in the Auditable Events table*].

Application Note: It is not feasible for the FIA_BLT_EXT.3 event to be audited if the rejection is performed at the HCI layer because the Bluetooth standard does not provide a notification interface for this behavior in the HCI. This is why the event is labeled as optional. However, if the rejection is performed above the HCI layer, it is expected that a conformant TOE should implement this functionality.

Evaluation Activities

FAU_GEN.1/BT
TSS
There are additional auditable events that serve to extend the FAU_GEN.1 SFR found in each Base-PP.

This SFR is evaluated in the same manner as defined by the Evaluation Activities for the claimed Base-PP. The only difference is that the evaluator shall also assess the auditable events required for this PP-Module in addition to those defined in the claimed Base-PP.

5.3.2 Cryptographic Support (FCS)

FCS_CKM_EXT.8 Bluetooth Key Generation

FCS_CKM_EXT.8.1

The TSF shall generate public/private ECDH key pairs every [**assignment**: *frequency of and/or criteria for new key pair generation*].

Application Note: There are multiple acceptable ways of keeping ECDH key pairs adequately fresh, including a time-based approach such that the same key pairs will not be used for more than, for instance, 24 hours. Alternatively, the criteria might be linked to the number of passed or failed authentication attempts. As a starting point to determine reasonable authentication attempt-based replacement criteria, note that the Bluetooth specification (v4.1, Vol. 2, 5.1) suggests mitigating repeated authentication attempts by changing a device's private key after three failed authentication attempts from any BD_ADDR, after ten successful pairings from any BD_ADDR, or after a combination of these such that any three successful pairings count as one failed pairing.

This requirement also applies to Bluetooth LE if the TOE supports LE Secure Connections, which was introduced in version 4.2 of the specification.

Evaluation Activities

FCS_CKM_EXT.8
TSS
The evaluator shall ensure that the TSS describes the criteria used to determine the frequency of generating new ECDH public/private key pairs. In particular, the evaluator shall ensure that the implementation does not permit the use of static ECDH key pairs.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following steps:
Step 1: Pair the TOE to a remote Bluetooth device and record the public key currently in use by the TOE. (This public key can be obtained using a Bluetooth protocol analyzer to inspect packets exchanged during pairing.)
Step 2: Perform necessary actions to generate new ECDH public/private key pairs. (Note that this test step depends on how the TSS describes the criteria used to determine the frequency of generating new ECDH public/private key pairs.)
Step 3: Pair the TOE to a remote Bluetooth device and again record the public key currently in use by the TOE.
Step 4: Verify that the public key in Step 1 differs from the public key in Step 3.

5.3.3 Identification and Authentication (FIA)

FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.1.1

The TSF shall require explicit user authorization before pairing with a remote Bluetooth device.

Application Note: User authorization includes explicit actions like affirming the remote device's name, expressing an intent to connect to the remote device, and entering relevant pairing information (e.g. PINs; numeric codes; or "yes/no" responses). The user must have to explicitly permit all pairing attempts; even when bonding is not taking place.

Because explicit user action must be required to permit pairing; it must not be possible for applications to programmatically enter pairing information (e.g. PINs; numeric codes; or "yes/no" responses) during the pairing process. The absence of public APIs for programmatic authorization is not sufficient to meet this requirement; hidden or private APIs must be absent as well.

Evaluation Activities

FIA_BLT_EXT.1
TSS
The evaluator shall examine the TSS to ensure that it contains a description of when user permission is required for Bluetooth pairing; and that this description mandates explicit user authorization via manual input for all Bluetooth pairing; including application use of the Bluetooth trusted channel and situations where temporary (non-bonded) connections are formed.

Guidance
The evaluator shall examine the API documentation provided as a means of satisfying the requirements for the ADV assurance class (see section 5.2.2 in the MDF PP and GPOS PP) and verify that this API documentation does not include any API for programmatic entering of pairing information (e.g. PINs; numeric codes; or "yes/no" responses) intended to bypass manual user input during pairing.

The evaluator shall examine the guidance to verify that these user authorization screens are clearly identified and instructions are given for authorizing Bluetooth pairings.

Tests
The evaluator shall perform the following steps:
Step 1: Initiate pairing with the TOE from a remote Bluetooth device that requests no man-in-the-middle protection; no bonding; and claims to have NoInput/NoOutput (IO) capability. Such a device will attempt to evoke behavior from the TOE that represents the minimal level of user interaction that the TOE supports during pairing.
Step 2: Verify that the TOE does not permit any Bluetooth pairing without explicit authorization from the user (e.g. the user must have to minimally answer "yes" or "allow" in a prompt).

FIA_BLT_EXT.2 Bluetooth Mutual Authentication

FIA_BLT_EXT.2.1

The TSF shall require Bluetooth mutual authentication between devices prior to any data transfer over the Bluetooth link.

Application Note: If devices are not already paired, the pairing process must be initiated. If the devices are already paired, mutual authentication based on the current link key must succeed before any data passes over the link.

Evaluation Activities

FIA_BLT_EXT.2
TSS
The evaluator shall ensure that the TSS describes how data transfer of any type is prevented before the Bluetooth pairing is completed. The TSS shall specifically call out any supported RFCOMM and L2CAP data transfer mechanisms. The evaluator shall ensure that the data transfers are only completed after the Bluetooth devices are paired and mutually authenticated.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall use a Bluetooth tool to attempt to access TOE files using the OBEX Object Push service (OBEX Push) and verify that pairing and mutual authentication are required by the TOE before allowing access. If the OBEX Object Push service is unsupported on the TOE; a different service that transfers data over Bluetooth L2CAP and/or RFCOMM may be used in this test.

FIA_BLT_EXT.3 Rejection of Duplicate Bluetooth Connections

FIA_BLT_EXT.3.1

The TSF shall discard pairing and session initialization attempts from a Bluetooth device address (BD_ADDR) to which an active session already exists.

Application Note: Session is defined as the time interval for which the TSF is actively connected to another device. Thus, the session terminates when the device disconnects from the TSF. If the TOE has an active session to a remote Bluetooth device, new session initialization and/or pairing attempts from devices claiming the same Bluetooth device address may be malicious and should be rejected/ignored. Only one session to a single remote BD_ADDR may be supported at a time.

Evaluation Activities

FIA_BLT_EXT.3
TSS
The evaluator shall ensure that the TSS describes how Bluetooth sessions are maintained such that at least two devices with the same Bluetooth device address are not simultaneously connected and such that the initial session is not superseded by any following session initialization attempts.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following steps:
Step 1: Pair the TOE with a remote Bluetooth device (DEV1) with a known address BD_ADDR. Establish an active session between the TOE and DEV1 with the known address BD_ADDR.
Step 2: Attempt to pair a second remote Bluetooth device (DEV2) claiming to have a Bluetooth device address matching DEV1 BD_ADDR to the TOE. Using a Bluetooth protocol analyzer, verify that the pairing attempt by DEV2 is not completed by the TOE and that the active session to DEV1 is unaffected.
Step 3: Attempt to initialize a session to the TOE from DEV2 containing address DEV1 BD_ADDR. Using a Bluetooth protocol analyzer, verify that the session initialization attempt by DEV2 is ignored by the TOE and that the initial session to DEV1 is unaffected.

FIA_BLT_EXT.4 Secure Simple Pairing

FIA_BLT_EXT.4.1

The TOE shall support Bluetooth Secure Simple Pairing, both in the host and the controller.

FIA_BLT_EXT.4.2

The TOE shall support Secure Simple Pairing during the pairing process.

Application Note: The Bluetooth host and controller each support a particular version of the Bluetooth Core Specification and a particular set of features. Support for various features is indicated by each side during the Link Manager Protocol (LMP) Features Exchange. Refer to the Bluetooth specification [Bluetooth] for feature definitions, including the definitions of Secure Simple Pairing (Controller Support) and Secure Simple Pairing (Host Support).

Evaluation Activities

FIA_BLT_EXT.4
TSS
The evaluator shall verify that the TSS describes the secure simple pairing process.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following steps:
Step 1: Initiate pairing with the TOE from a remote Bluetooth device that supports Secure Simple Pairing.
Step 2: During the pairing process; observe the packets in a Bluetooth protocol analyzer and verify that the TOE claims support for both "Secure Simple Pairing (Host Support)" and "Secure Simple Pairing (Controller Support)" during the LMP Features Exchange.
Step 3: Verify that Secure Simple Pairing is used during the pairing process.

FIA_BLT_EXT.6 Trusted Bluetooth Device User Authorization

FIA_BLT_EXT.6.1

The TSF shall require explicit user authorization before granting trusted remote devices access to services associated with the following Bluetooth profiles: [**assignment**: *list of Bluetooth profiles*].

Application Note: In addition to pairing, it may be appropriate to require explicit user action to authorize a particular remote device to access certain Bluetooth services. The TSF may choose to require this additional action for all devices or only for those devices that do not have a required level of trust.
It is strongly preferred that for each device, the TSF maintains a list of devices trusted to use for that particular service. However, the TSF might designate certain devices as having a trusted device relationship with the TOE and granting them "blanket" access to all services.

Furthermore, it may be the case that the TSF allows movement of devices from the untrusted to the trusted category for a particular service after the user provides explicit authorization for the device to use the service. For example, it may be appropriate to require that the user provide explicit, manual authorization before a remote device may use the OBEX service for an object transfer the first time. The user might be given the option to permit future connections to that service by the particular device without requiring explicit authorization each time.

Evaluation Activities

FIA_BLT_EXT.6
TSS
The evaluator shall verify that the TSS describes all Bluetooth profiles and associated services for which explicit user authorization is required before a remote device can gain access. The evaluator shall also verify that the TSS describes any difference in behavior based on whether or not the device has a trusted relationship with the TOE for that service (i.e. whether there are any services that require explicit user authorization for untrusted devices that do not require such authorization for trusted devices). The evaluator shall also verify that the TSS describes the method by which a device can become 'trusted'.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following tests:

- *Test 1: While the service is in active use by an application on the TOE, the evaluator shall attempt to gain access to a "protected" Bluetooth service (as specified in the assignment in FIA_BLT_EXT.6.1) from a "trusted" remote device. The evaluator shall verify that the user is explicitly asked for authorization by the TOE to allow access to the service for the particular remote device. The evaluator shall deny the authorization on the TOE and verify that the remote attempt to access the service fails due to lack of authorization.*
- *Test 2: The evaluator shall repeat Test 1, this time allowing the authorization and verifying*

that the remote device successfully accesses the service.

FIA_BLT_EXT.7 Untrusted Bluetooth Device User Authorization

FIA_BLT_EXT.7.1

The TSF shall require explicit user authorization before granting untrusted remote devices access to services associated with the following Bluetooth profiles: [**assignment**: *list of Bluetooth profiles*].

Application Note: FIA_BLT_EXT.7 differs from FIA_BLT_EXT.6 because a conformant TOE may distinguish between "trusted" and "untrusted" devices such that the TSF grants "untrusted" devices access to fewer services following pairing. However, this behavior is not required; if the TSF does not treat "trusted" and "untrusted" devices any differently, the ST author may complete the assignments in FIA_BLT_EXT.6.1 and FIA_BLT_EXT.7.1 with lists of Bluetooth profiles.

Evaluation Activities

FIA_BLT_EXT.7
TSS
The TSS evaluation activities for this component are addressed by FIA_BLT_EXT.6.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following tests if the TSF differentiates between "trusted" and "untrusted" devices for the purpose of granting access to services. If it does not, then the test evaluation activities for FIA_BLT_EXT.6 are sufficient to satisfy this component.

- *Test 3: While the service is in active use by an application on the TOE, the evaluator shall attempt to gain access to a "protected" Bluetooth service (as specified in the assignment in FIA_BLT_EXT.7.1) from an "untrusted" remote device. The evaluator shall verify that the user is explicitly asked for authorization by the TOE to allow access to the service for the particular remote device. The evaluator shall deny the authorization on the TOE and verify that the remote attempt to access the service fails due to lack of authorization.*
- *Test 4: The evaluator shall repeat Test 1, this time allowing the authorization and verifying that the remote device successfully accesses the service.*
- *Test 5: (conditional): If there exist any services that require explicit user authorization for access by untrusted devices but not by trusted devices (i.e. a service that is listed in FIA_BLT_EXT.7.1 but not FIA_BLT_EXT.6.1), the evaluator shall repeat Test 1 for these services and observe that the results are identical. That is, the evaluator shall use these results to verify that explicit user approval is required for an untrusted device to access these services, and failure to grant this approval will result in the device being unable to access them.*
- *Test 6: (conditional): If test 3 applies, the evaluator shall repeat Test 2 using any services chosen in Test 3 and observe that the results are identical. That is, the evaluator shall use these results to verify that explicit user approval is required for an untrusted device to access these services, and granting this approval will result in the device being able to access them.*
- *Test 7: (conditional): If test 3 applies, the evaluator shall repeat Test 3 except this time designating the device as "trusted" prior to attempting to access the service. The evaluator shall verify that access to the service is granted without explicit user authorization (because the device is now trusted and therefore FIA_BLT_EXT.7.1 no longer applies to it). That is, the evaluator shall use these results to demonstrate that the TSF will grant a device access to different services depending on whether or not the device is trusted.*

5.3.4 Trusted Path/Channels (FTP)

FTP_BLT_EXT.1 Bluetooth Encryption

FTP_BLT_EXT.1.1

The TSF shall enforce the use of encryption when transmitting data over the Bluetooth trusted channel for BR/EDR and [**selection**: *LE, no other connections*].

Application Note: LE is selectable because not all conformant TOEs include support for LE. If LE is supported, it is expected that the TSF be able to provide encryption for this interface. Selection of LE in FTP_BLT_EXT.1.1 requires the inclusion of the selection-based SFR FTP_BLT_EXT.3/LE.

FTP_BLT_EXT.1.2

The TSF shall use key pairs per FCS_CKM_EXT.8 for Bluetooth encryption.

Evaluation Activities

FTP_BLT_EXT.1
TSS
The evaluator shall verify that the TSS describes the use of encryption, the specific Bluetooth protocol(s) it applies to, and whether it is enabled by default.

The evaluator shall verify that the TSS includes the protocol used for encryption of the transmitted data and the key generation mechanism used.

Guidance
The evaluator shall verify that the operational guidance includes instructions on how to configure the TOE to require the use of encryption during data transmission (unless this behavior is enforced by default).

Tests
There are no test EAs for this component. Testing for this SFR is addressed through the evaluation of FTP_BLT_EXT.3/BR and, if claimed, FTP_BLT_EXT.3/LE.

FTP_BLT_EXT.2 Persistence of Bluetooth Encryption

FTP_BLT_EXT.2.1

The TSF shall [**selection**: *restart encryption*, *terminate the connection*] if the remote device stops encryption while connected to the TOE.

Application Note: Permitting devices to terminate and/or restart encryption in the middle of a connection weakens user data protection. Note that an encryption pause request, which includes a request to stop encryption, stops encryption only temporarily. This requirement is not intended to address the encryption pause feature.

Evaluation Activities

FTP_BLT_EXT.2
TSS
The evaluator shall verify that the TSS describes the TSF's behavior if a remote device stops encryption while connected to the TOE.

Guidance
The evaluator shall verify that the operational guidance describes how to enable/disable encryption (if configurable).

Tests
The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:
Step 1: Initiate pairing with the TOE from a remote Bluetooth device that has been configured to have a minimum encryption key size that is equal to or greater than that of the TOE.
Step 2: After pairing has successfully finished and while a connection exists between the TOE and the remote device; turn off encryption on the remote device. This can be done using commercially-available tools.
Step 3: Verify that the TOE either restarts encryption with the remote device or terminates the connection with the remote device.

FTP_BLT_EXT.3 Bluetooth Encryption Parameters

FTP_BLT_EXT.3.1

The TSF shall set the minimum encryption key size to [**assignment**: *key size larger than or equal to 128 bits*] for [**assignment**: *Bluetooth protocol*].

FTP_BLT_EXT.3/BR Bluetooth Encryption Parameters (BR/EDR)

FTP_BLT_EXT.3.1/BR

The TSF shall set the minimum encryption key size to [**assignment**: *key size larger than or equal to 128 bits*] for [*BR/EDR*] and not negotiate encryption key sizes smaller than the minimum size.

Application Note: Encryption is mandatory for BR/EDR connections when both devices support Secure Simple Pairing. Minimum encryption requirements will be set and verified for each Bluetooth profile/application.

Evaluation Activities

FTP_BLT_EXT.3/BR

TSS
The evaluator shall examine the TSS and verify that it specifies the minimum key size for BR/EDR encryption, whether this value is configurable, and the mechanism by which the TOE will not negotiate keys sizes smaller than the minimum.

Guidance
The evaluator shall verify that the guidance includes instructions on how to configure the minimum encryption key size for BR/EDR encryption, if configurable.

Tests
The evaluator shall perform the following tests:

- *Test 8: The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:*
  Step 1: Initiate BR/EDR pairing with the TOE from a remote Bluetooth device that has been configured to have a minimum encryption key size that is equal to or greater than that of the TOE. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.
  Step 2: Use a Bluetooth packet sniffer to verify that the encryption key size negotiated for the connection is at least as large as the minimum encryption key size defined for the TOE.
- *Test 9: (conditional): If the encryption key size is configurable, configure the TOE to support a different minimum key size, then repeat Test 1 and verify that the negotiated key size is at least as large as the new minimum value.*
- *Test 10: The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:*
  Step 1: Initiate BR/EDR pairing with the TOE from a remote Bluetooth device that has been configured to have a maximum encryption key size of 1 byte. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.
  Step 2: Verify that the encryption key size suggested by the remote device is not accepted by the TOE and that the connection is not completed.

5.4 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 3: SFR Rationale

Objective	Addressed by	Rationale
O.PROTECTED_COMMS	FIA_BLT_EXT.1	FIA_BLT_EXT.1 supports the objective by ensuring that Bluetooth communications are not initiated without user approval.
	FIA_BLT_EXT.2	FIA_BLT_EXT.2 supports the objective by requiring the TSF to implement Bluetooth mutual authentication.
	FIA_BLT_EXT.3	FIA_BLT_EXT.3 supports the objective by preventing Bluetooth spoofing by rejecting connections with duplicate device addresses.
	FIA_BLT_EXT.4	FIA_BLT_EXT.4 supports the objective by defining the TSF's implementation of Bluetooth Secure Simple Pairing.
	FIA_BLT_EXT.5	FIA_BLT_EXT.5 supports the objective by requiring the TSF to support Secure Connections Only mode for the supported Bluetooth communication channels.
	FIA_BLT_EXT.6	FIA_BLT_EXT.6 supports the objective by requiring the TSF to specify the Bluetooth profiles that it requires explicit user authorization to grant access to for trusted devices.
	FTP_BLT_EXT.1	FTP_BLT_EXT.1 supports the objective by requiring the TSF to implement encryption to protect Bluetooth communications
	FTP_BLT_EXT.2	FTP_BLT_EXT.2 supports the objective by requiring the TSF to prevent data transmission over Bluetooth if the paired device is not using encryption.

6 Consistency Rationale

6.1 Protection Profile for Bluetooths

6.1.1 Consistency of TOE Type

If this PP-Module is used to extend the MDF PP, the TOE type for the overall TOE is still a mobile device. However, one of the functions of the device must be the ability for it to have Bluetooth capability. The TOE boundary is simply extended to include that functionality.

6.1.2 Consistency of Security Problem Definition

The threats that apply to this PP-Module are inherited from the Base-PP to which the TOE also conforms. This PP-Module does not add or remove any elements to the security problem definition given in the MDF PP.

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.NETWORK_EAVESDROP	This threat comes directly from both base PPs.
T.NETWORK_ATTACK	This threat comes directly from both base PPs.

6.1.3 Consistency of Objectives

The objectives that apply to this PP-Module are inherited from the Base-PP to which the TOE also conforms. This PP-Module does not add or remove any elements to the objectives given in the MDF PP. The objectives for the TOEs are consistent with the Bluetooths PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.PROTECTED_COMMS	This objective comes directly from the PP.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the Bluetooths PP that are needed to support Bluetooth functionality. This is considered to be consistent because the functionality provided by the Bluetooths PP is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the Bluetooths PP as well as new SFRs that are used entirely to provide functionality for Bluetooths. The rationale for why this does not conflict with the claims defined by the Bluetooths PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FMT_SMF_EXT.1	This SFR is unchanged from its definition in the Base-PP; the only change required by this PP-Module is how to interpret it in the context of Bluetooth capabilities.
Additional SFRs	
FMT_SMF_EXT.1/BT	The ST author is instructed to complete an assignment in the SFR with information related to Bluetooth, and to include additional management functions in this SFR based on the Bluetooth capability defined by the PP-Module.
Mandatory SFRs	
FAU_GEN.1/BT	The PP-Module defines auditable events for Bluetooth that extends the audit functionality defined in each Base-PP.
FCS_CKM_EXT.8	
FIA_BLT_EXT.1	
FIA_BLT_EXT.2	
FIA_BLT_EXT.3	
FIA_BLT_EXT.4	
FIA_BLT_EXT.6	
FIA_BLT_EXT.7	
FTP_BLT_EXT.1	
FTP_BLT_EXT.2	
FTP_BLT_EXT.3/BR	
Optional SFRs	

This PP-Module does not define any Optional requirements.
Objective SFRs
FIA_BLT_EXT.5
Implementation-based SFRs
This PP-Module does not define any Implementation-based requirements.
Selection-based SFRs
FTP_BLT_EXT.3/LE

6.2 Protection Profile for Bluetooths

6.2.1 Consistency of TOE Type

If this PP-Module is used to extend the [GPOS PP], the TOE type for the overall TOE is still a generic operating system. However, one of the functions of the generic operating system must be the ability for it to have Bluetooth capability. The TOE boundary is simply extended to include that functionality.

6.2.2 Consistency of Security Problem Definition

The threats that apply to this PP-Module are inherited from the Base-PP to which the TOE also conforms. This PP-Module does not add or remove any elements to the security problem definition given in the GPOS PP.

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.NETWORK_EAVESDROP	This threat comes directly from both base PPs.
T.NETWORK_ATTACK	This threat comes directly from both base PPs.

6.2.3 Consistency of Objectives

The objectives that apply to this PP-Module are inherited from the Base-PP to which the TOE also conforms. This PP-Module does not add or remove any elements to the objectives given in the GPOS PP. The objectives for the TOEs are consistent with the Bluetooths PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.PROTECTED_COMMS	This objective comes directly from the PP.

6.2.4 Consistency of Requirements

This PP-Module identifies several SFRs from the Bluetooths PP that are needed to support Bluetooth functionality. This is considered to be consistent because the functionality provided by the Bluetooths PP is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the Bluetooths PP as well as new SFRs that are used entirely to provide functionality for Bluetooths. The rationale for why this does not conflict with the claims defined by the Bluetooths PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FMT_MOF_EXT.1	This SFR is unchanged from its definition in the Base-PP; the only change required by this PP-Module is how to interpret it in the context of Bluetooth capabilities.
FMT_SMF_EXT.1	This SFR is unchanged from its definition in the Base-PP; the only change required by this PP-Module is how to interpret it in the context of Bluetooth capabilities.
Additional SFRs	
FMT_MOF_EXT.1/BT	The ST author is required to associate all claimed management functions with the administrative privileges required to execute them. This PP-Module simply extends this requirement to apply to the management functions added and mandated by the PP-Module.
FMT_SMF_EXT.1/BT	The ST author is required to include an optional management function defined in the Base-PP that relates to Bluetooth, and to include additional management functions in this SFR based on the Bluetooth capability defined by the PP-Module.
Mandatory SFRs	
FAU_GEN.1/BT	The PP-Module defines auditable events for Bluetooth that extends the audit functionality defined in each Base-PP.
FCS_CKM_EXT.8	

FIA_BLT_EXT.1
FIA_BLT_EXT.2
FIA_BLT_EXT.3
FIA_BLT_EXT.4
FIA_BLT_EXT.6
FIA_BLT_EXT.7
FTP_BLT_EXT.1
FTP_BLT_EXT.2
FTP_BLT_EXT.3/BR
Optional SFRs
This PP-Module does not define any Optional requirements.
Objective SFRs
FIA_BLT_EXT.5
Implementation-based SFRs
This PP-Module does not define any Implementation-based requirements.
Selection-based SFRs
FTP_BLT_EXT.3/LE

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

This PP-Module does not define any Strictly Optional SFRs.

A.2 Objective Requirements

A.2.1 Identification and Authentication

FIA_BLT_EXT.5 Bluetooth Secure Connections

FIA_BLT_EXT.5.1

The TOE shall support Secure Connections Only mode for Bluetooth BR/EDR and [**selection**: *Bluetooth LE*, *no other Bluetooth protocol*].

Application Note: The specification states that Secure Connections Only Mode, also called "FIPS Mode," should be used when security is more important than backwards compatibility. From the specification, "The Host will enforce that the P-256 elliptic curve is used during pairing; the secure authentication sequences are used; and AES-CCM is used for encryption." Also, "if a BR/EDR/LE device is configured in Secure Connections Only Mode, then a transport will only be used when Secure Connections is supported by both devices."

Evaluation Activities

FIA_BLT_EXT.5
TSS
The evaluator shall ensure that the TSS describes support for Secure Connections Only mode for BR/EDR and, if supported, Bluetooth LE.

Guidance
The evaluator shall ensure that the guidance includes instructions on how to place the TOE into Secure Connections Only mode for BR/EDR and, if supported, Bluetooth LE.

Tests
The evaluator shall perform the following tests, once for BR/EDR and once for LE (if applicable):

- *Test 11: The evaluator shall place the TOE into Secure Connections Only mode. The evaluator shall then attempt a pairing to a remote device that does not support Secure Connections Only mode and verify that the attempt fails.*
- *Test 12: The evaluator shall place the TOE into Secure Connections Only mode. The evaluator shall attempt a pairing to a remote device that supports Secure Connections Only mode and has it enabled. The evaluator shall verify that the pairing attempt succeeds. The evaluator shall also use a Bluetooth packet sniffer to verify that the parameters of the pairing and encryption are consistent with Secure Connections.*

A.3 Implementation-based Requirements

This PP-Module does not define any Implementation-based SFRs.

Appendix B - Selection-based Requirements

B.1 Trusted Path/Channels

FTP_BLT_EXT.3/LE Bluetooth Encryption Parameters (LE)

The inclusion of this selection-based component depends upon selection in FTP_BLT_EXT.1.1.

FTP_BLT_EXT.3.1/LE

The TSF shall set the minimum encryption key size to [**assignment**: *key size larger than or equal to 128 bits*] for [*LE*] and not negotiate encryption key sizes smaller than the minimum size.

Application Note: The TOE must implement encryption for Bluetooth BR/EDR as required by FTP_BLT_EXT.1.1. A conformant TOE does not need to support Bluetooth LE; however, if it does, then it must also support encryption for it. FTP_BLT_EXT.3/LE must therefore be claimed if 'LE' is selected in FTP_BLT_EXT.1.1.

Evaluation Activities

FTP_BLT_EXT.3/LE
TSS
The evaluator shall examine the TSS and verify that it specifies the minimum key size for LE encryption, whether this value is configurable, and the mechanism by which the TOE will not negotiate keys sizes smaller than the minimum.

Guidance
The evaluator shall verify that the guidance includes instructions on how to configure the minimum encryption key size for LE encryption, if configurable.

Tests
The evaluator shall perform the following tests:

- *Test 13: The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:*
  Step 1: Initiate LE pairing with the TOE from a remote Bluetooth device that has been configured to have a minimum encryption key size that is equal to or greater than that of the TOE. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.
  Step 2: Use a Bluetooth packet sniffer to verify that the encryption key size negotiated for the connection is at least as large as the minimum encryption key size defined for the TOE.
- *Test 14: (conditional): If the encryption key size is configurable, configure the TOE to support a different minimum key size, then repeat Test 1 and verify that the negotiated key size is at least as large as the new minimum value.*
- *Test 15: The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:*
  Step 1: Initiate LE pairing with the TOE from a remote Bluetooth device that has been configured to have a maximum encryption key size of 1 byte. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.
  Step 2: Verify that the encryption key size suggested by the remote device is not accepted by the TOE and that the connection is not completed.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 4: Extended Component Definitions

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_CKM_EXT Cryptographic Key Management
Identification and Authentication (FIA)	FIA_BLT_EXT Bluetooth Pairing
Trusted Path/Channels (FTP)	FTP_BLT_EXT Bluetooth Trusted Communications

C.2 Extended Component Definitions

C.2.1 Cryptographic Support (FCS)

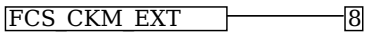
This PP-Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

C.2.1.1 FCS_CKM_EXT Cryptographic Key Management

Family Behavior

Components in this family define requirements for cryptographic key management beyond those which are specified in the Part 2 family FCS_CKM.

Component Leveling



FCS_CKM_EXT.8, Bluetooth Key Generation, requires the TSF to generate key pairs used for Bluetooth over a specified time period or in response to some observed event.

Management: FCS_CKM_EXT.8

No specific management functions are identified.

Audit: FCS_CKM_EXT.8

There are no auditable events foreseen.

FCS_CKM_EXT.8 Bluetooth Key Generation

Hierarchical to: No other components.

Dependencies to: FCS_CKM.1 Cryptographic Key Generation
FPT_STM.1 Reliable Time Stamps
FTP_BLT_EXT.1 Bluetooth Encryption

FCS_CKM_EXT.8.1

The TSF shall generate public/private ECDH key pairs every [**assignment**: *frequency of and/or criteria for new key pair generation*].

C.2.2 Identification and Authentication (FIA)

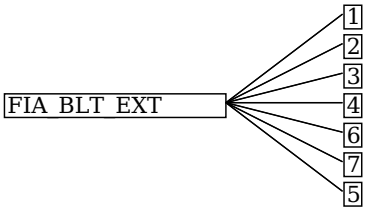
This PP-Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

C.2.2.1 FIA_BLT_EXT Bluetooth Pairing

Family Behavior

Components in this family define Bluetooth-specific identification and authentication requirements.

Component Leveling



FIA_BLT_EXT.1, Bluetooth User Authorization, requires the TSF to have explicit user authorization before allowing a Bluetooth pairing.

FIA_BLT_EXT.2, Bluetooth Mutual Authentication, requires the TSF to enforce mutual authentication for Bluetooth.

FIA_BLT_EXT.3, Rejection of Duplicate Bluetooth Connections, requires the TSF to reject duplicate attempts to connect to Bluetooth.

FIA_BLT_EXT.4, Secure Simple Pairing, requires the TSF to support Secure Simple Pairing.

FIA_BLT_EXT.6, Trusted Bluetooth Device User Authorization, requires the TSF to have explicit user authentication before associating trusted services with Bluetooth.

FIA_BLT_EXT.7, Untrusted Bluetooth Device User Authorization, requires the TSF to have explicit user authentication before associating untrusted services with Bluetooth.

FIA_BLT_EXT.5, Bluetooth Secure Connections, requires the TSF to support Secure Connections Only mode.

Management: FIA_BLT_EXT.1

No specific management functions are identified.

Audit: FIA_BLT_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Failed user authorization of Bluetooth device.
- Failed user authorization for local Bluetooth device.

FIA_BLT_EXT.1 Bluetooth User Authorization

Hierarchical to: No other components.

Dependencies to: No dependencies.

FIA_BLT_EXT.1.1

The TSF shall require explicit user authorization before pairing with a remote Bluetooth device.

Management: FIA_BLT_EXT.2

No specific management functions are identified.

Audit: FIA_BLT_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Initiation of Bluetooth connection.
- Failure of Bluetooth connection.

FIA_BLT_EXT.2 Bluetooth Mutual Authentication

Hierarchical to: No other components.

Dependencies to: FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.2.1

The TSF shall require Bluetooth mutual authentication between devices prior to any data transfer over the Bluetooth link.

Management: FIA_BLT_EXT.3

No specific management functions are identified.

Audit: FIA_BLT_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Duplicate connection attempt.

FIA_BLT_EXT.3 Rejection of Duplicate Bluetooth Connections

Hierarchical to: No other components.

Dependencies to: FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.3.1

The TSF shall discard pairing and session initialization attempts from a Bluetooth device address (BD_ADDR) to which an active session already exists.

Management: FIA_BLT_EXT.4

No specific management functions are identified.

Audit: FIA_BLT_EXT.4

There are no auditable events foreseen.

FIA_BLT_EXT.4 Secure Simple Pairing

Hierarchical to: No other components.

Dependencies to: FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.4.1

The TOE shall support Bluetooth Secure Simple Pairing, both in the host and the controller.

FIA_BLT_EXT.4.2

The TOE shall support Secure Simple Pairing during the pairing process.

Management: FIA_BLT_EXT.6

The following actions could be considered for the management functions in FMT:

- Ability to specify the services that require explicit user authorization before trusted devices can use them.

Audit: FIA_BLT_EXT.6

There are no auditable events foreseen.

FIA_BLT_EXT.6 Trusted Bluetooth Device User Authorization

Hierarchical to: No other components.

Dependencies to: FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.6.1

The TSF shall require explicit user authorization before granting trusted remote devices access to services associated with the following Bluetooth profiles: [**assignment**: *list of Bluetooth profiles*].

Management: FIA_BLT_EXT.7

The following actions could be considered for the management functions in FMT:

- Ability to specify the services that require explicit user authorization before untrusted devices can use them.

Audit: FIA_BLT_EXT.7

There are no auditable events foreseen.

FIA_BLT_EXT.7 Untrusted Bluetooth Device User Authorization

Hierarchical to: No other components.

Dependencies to: FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.7.1

The TSF shall require explicit user authorization before granting untrusted remote devices access to services associated with the following Bluetooth profiles: [**assignment**: *list of Bluetooth profiles*].

Management: FIA_BLT_EXT.5

No specific management functions are identified.

Audit: FIA_BLT_EXT.5

There are no auditable events foreseen.

FIA_BLT_EXT.5 Bluetooth Secure Connections

Hierarchical to: No other components.

Dependencies to: FIA_BLT_EXT.1 Bluetooth User Authorization

FIA_BLT_EXT.5.1

The TOE shall support Secure Connections Only mode for Bluetooth BR/EDR and [**selection**: *Bluetooth LE, no other Bluetooth protocol*].

C.2.3 Trusted Path/Channels (FTP)

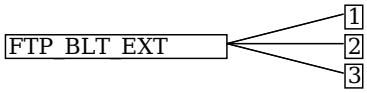
This PP-Module defines the following extended components as part of the FTP class originally defined by CC Part 2:

C.2.3.1 FTP_BLT_EXT Bluetooth Trusted Communications

Family Behavior

Components in this family define requirements for Bluetooth encryption.

Component Leveling



FTP_BLT_EXT.1, Bluetooth Encryption, requires the TSF to enforce encryption when transmitting over Bluetooth.

FTP_BLT_EXT.2, Persistence of Bluetooth Encryption, requires the TSF to ensure encryption for the duration of the use of the Bluetooth channel.

FTP_BLT_EXT.3, Bluetooth Encryption Parameters, specifies the key sizes used for Bluetooth.

Management: FTP_BLT_EXT.1

No specific management functions are identified.

Audit: FTP_BLT_EXT.1

There are no auditable events foreseen.

FTP_BLT_EXT.1 Bluetooth Encryption

Hierarchical to: No other components.

Dependencies to: FCS_CKM_EXT.8 Bluetooth Key Generation
FIA_BLT_EXT.1 Bluetooth User Authorization

FTP_BLT_EXT.1.1

The TSF shall enforce the use of encryption when transmitting data over the Bluetooth trusted channel for BR/EDR and [**assignment**: *list of other connection modes*].

FTP_BLT_EXT.1.2

The TSF shall use key pairs per FCS_CKM_EXT.8 for Bluetooth encryption.

Management: FTP_BLT_EXT.2

No specific management functions are identified.

Audit: FTP_BLT_EXT.2

There are no auditable events foreseen.

FTP_BLT_EXT.2 Persistence of Bluetooth Encryption

Hierarchical to: No other components.

Dependencies to: FTP_BLT_EXT.1 Bluetooth Encryption

FTP_BLT_EXT.2.1

The TSF shall [**selection**: *restart encryption*, *terminate the connection*] if the remote device stops encryption while connected to the TOE.

Management: FTP_BLT_EXT.3

The following actions could be considered for the management functions in FMT:

- Specification of minimum encryption key size.

Audit: FTP_BLT_EXT.3

There are no auditable events foreseen.

FTP_BLT_EXT.3 Bluetooth Encryption Parameters

Hierarchical to: No other components.

Dependencies to: FTP_BLT_EXT.1 Bluetooth Encryption

FTP_BLT_EXT.3.1

The TSF shall set the minimum encryption key size to [**assignment**: *key size larger than or equal to 128 bits*] for [**assignment**: *Bluetooth protocol*].

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. However, these requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.2 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

Requirement	Rationale for Satisfaction
FCS_CKM.1 - Cryptographic Key Generation	FCS_CKM_EXT.8 has a dependency on FCS_CKM.1 for the generation of ECDH key pairs. This dependency is implicitly satisfied in this PP-Module because both Base-PPs the PP-Module is intended to extend define this SFR and specify ECDH key generation as a required capability of the TOE. Therefore, a conformant TOE will always have this capability.
FPT_STM.1 - Reliable Time Stamps	FCS_CKM_EXT.8 has a dependency on FPT_STM.1 because key generation may be triggered by a given time period elapsing. When the TOE claims conformance to [MDF], this dependency is satisfied explicitly through the Base-PP's definition of FPT_STM.1. When the TOE claims conformance to [GPOS], this dependency is satisfied implicitly through that PP's A.PLATFORM assumption of a trustworthy computing platform, which can be reasonably assumed to include a hardware real-time clock.

Appendix E - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the Base-PPs.

Appendix F - Acronyms

Acronym	Meaning
ACL	Asynchronous Connection-Less
AES	Advanced Encryption Standard
AES-CCM	AES Counter with CBC-MAC Mode
AFH	Adaptive Frequency Hopping
API	Application Programming Interface
Base-PP	Base Protection Profile
BR	Basic Rate
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
ECDH	Elliptic Curve Diffie-Hellman
EDR	Enhanced Data Rate
EP	Extended Package
FP	Functional Package
FTP	File Transfer Protocol
HCI	Host Controller Interface
L2CAP	Logical Link Control and Adaptation Protocol
LE	Low Energy
LMP	Link Manager Protocol
MDF	Mobile Device Fundamentals
OBEX	Object Exchange
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

Appendix G - Bibliography

Identifier	Title
[Bluetooth]	Bluetooth Core Specifications, version 5.2; December 2019,
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Evaluation Methodology for Information Technology Security - Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017.
[GPOS]	Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
[MDF]	Protection Profile for Mobile Device Fundamentals, Version 3.2, April 15, 2021