Supporting Document
Mandatory Technical Document

PP-Module for Bluetooth
Version: 1.0
2021-04-15
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2021-04-15	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Bluetooth products.

Acknowledgments:
This SD was developed with support from NIAP Bluetooth Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Bluetooth is to describe the security functionality of Bluetooth products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PPs:

- Protection Profile for Mobile Devices, Version
- Protection Profile for General Purpose Operating Systems, Version

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Bluetooth, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 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 Protection Profiles.
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.

1.3.2 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 Device	A device that has a fixed relationship with another device and has full access to all services.
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.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator’s verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary

evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for Mobile Devices

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the Mobile Devices PP.

2.1.1 Modified SFRs

2.1.1.1 Security Management (FMT)

FMT_SMF_EXT.1 Specification of Management Functions

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

2.1.2 Additional SFRs

2.1.2.1 Security Management (FMT)

FMT_SMF_EXT.1/BT Specification of Management Functions

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.

2.2 Protection Profile for General Purpose Operating Systems

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the General Purpose Operating Systems PP.

2.2.1 Modified SFRs

2.2.1.1 Security Management (FMT)

FMT_MOF_EXT.1 Management of Security Functions Behavior

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

2.2.2 Additional SFRs

2.2.2.1 Security Management (FMT)

FMT_MOF_EXT.1/BT Management of Security Functions Behavior

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/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:

2.3 TOE SFR Evaluation Activities

2.3.1 Security Audit (FAU)

FAU_GEN.1/BT Audit Data Generation (Bluetooth)

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.

2.3.2 Cryptographic Support (FCS)

FCS_CKM_EXT.8 Bluetooth Key Generation

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.

2.3.3 Identification and Authentication (FIA)

FIA_BLT_EXT.1 Bluetooth User Authorization

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
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
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
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
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
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 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.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 2:** The evaluator shall repeat Test 1, this time allowing the authorization and verifying that the remote device successfully accesses the service.
- **Test 3:** (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 4:** (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 5:** (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.

2.3.4 Trusted Path/Channels (FTP)

FTP_BLT_EXT.1 Bluetooth Encryption

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
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/BR Bluetooth Encryption Parameters (BR/EDR)

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 1:** 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 2:** (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 3:** 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.

2.4 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.5 Evaluation Activities for Selection-Based SFRs

2.5.1 Trusted Path/Channels

FTP_BLT_EXT.3/LE Bluetooth Encryption Parameters (LE)

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 1:** 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 2:** (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 3:** 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.

2.6 Evaluation Activities for Objective SFRs

2.6.1 Identification and Authentication

FIA_BLT_EXT.5 Bluetooth Secure Connections

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 1:** 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 2:** 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.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base-PP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against the Base-PP as well. The Base-PP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the chosen Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

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