BLUETOOTH® DOC	Date / Year-Month-Day 2011-12-27	Approved Adopted	Revision V10r00	Document No HOGP_SPEC
Prepared By HID WG	E-mail Address hid-main@bluetooth.org			N.B.

HID OVER GATT PROFILE SPECIFICATION

Abstract

This profile defines how a device with *Bluetooth* low energy wireless communications can support HID services over the *Bluetooth* low energy protocol stack using the Generic Attribute Profile.

Revision History

Revision	Date	Comments
D09r01	2011-06-30	First Draft of LE HID Profile
D09r02	2011-07-05	Review comments from Alain Michaud and Jacques Chassot
D09r03	2011-07-08	Updated the review comments, HID Flags and added Appendix A
D09r04	2011-07-15	Revised section 0 to clarify device-initiated and host-initiated connection establishment
D09r05	2011-07-15	Sandeep Kamath updated text in sections 5.1.2 and 5.2.6, fixed Idle Connection Timeout references
D09r06	2011-07-21	Updated at HID WG F2F, Malmö
D09r07	2011-08-04	Changes for Option 1a
D09r08	2011-08-09	Added section 4.3.1.5
D09r09	2011-08-10	Added review comments and renamed “Flags” to “Information”
D09r10	2011-08-11	Added review comments
D09r11	2011-08-11	Added more comments
D09r12	2011-08-12	Updates from HID WG CC, 2011-08-11
D09r13	2011-08-17	Removed addressed comments, added a few editorial changes
D09r14	2011-08-17	Added comments from Chris Church and Mike Tsai
D09r15	2011-08-19	Resolved comments
D09r16	2011-08-22	Removed soft/hard reset commands
D09r17	2011-08-26	Updated section 5.1.3, removed addressed comments
D09r18	2011-08-29	Revision Revoked
D09r19	2011-09-05	Clean version
D09r20	2011-09-06	Changed Boot Mode only Hosts
D09r21	2011-09-07	Added more details on Boot Mode only Hosts
D09r22	2011-09-08	Added recommendation for DIS C1 values.
D09r23	2011-09-10	Added review comments
D09r24	2011-09-12	Accepted review comments and changed Tables 4-1 and 4-2 to accommodate clarified requirements. Added to sections 3.1 through 3.4 to clarify additional security requirements beyond Service Specs
D09r25	2001-09-13	Changes to accommodate HID Boot Report Mapping as a characteristic, including updating Tables 4-1 and Table 4-2, adding new characteristic and GATT sub-proc. Rationalized conditionals in Tables 4-1 and 4-2. Updated section 4.2 updated Security Considerations in s6.1.
D09r26	2011-09-13	Updated table 6-1. Updated references section
D09r27	2011-09-14	Added new subsections to 3.1, 3.2, 3.3, 3.4 to define Service Types & reformatted subsections
D09r28	2011-09-14	Addressed review comments, changed all instances of Report Mode to Report Protocol Mode and all instances of Boot Mode to Boot Protocol Mode. Inserted table of Figures and List of Tables. Changed section 4.2.2.1 to separate Service & Characteristic discovery for Boot Protocol Mode Hosts. Issued clean version
D09r29	2011-09-16	Updates from HID WG CC 2011-09-15
D09r30	2011-09-16	Formatting edits, changed HID Report to HID Control Point in section 4.8

Revision	Date	Comments
D09r31	2011-09-17	Updated section 4.8 for Get Protocol Mode
D09r32	2011-09-19	Addressed review comments from Jacques Chassot
D09r33	2011-09-20	Corrected references column in Table 4-1
D09r34	2011-09-26	Renamed to HID over GATT
D09r35	2011-09-29	Reverted some low energy deletions, added HID State, addressed Tim and Randy's comments.
D09r36	2011-09-29	Added HID Protocol Mode, removed get/set protocol from HID Control Point. Comments addressed from HID WG CC
D09r37	2011-10-09	Updates from the Budapest F2F
D09r38	2011-10-15	Added details on Translation Layer, Report Instance characteristic descriptor and External Report Reference characteristic descriptor.
D09r39	2011-10-15	Updated following redesign of HID Service after BARB review. Removed Report Reference characteristic descriptor from Report Map characteristic and into Report (or non-HID Service characteristics). Added External Report Reference characteristic descriptor. Multiple HID Services allowed. Mandated including external services with characteristics described in Report Map.
D09r40	2011-10-25	Updated to match HID Service r38 (removed Boot Report Reference characteristic, added Boot Keyboard Input Report, Boot Keyboard Output Report, and Boot Mouse Input Report).
D09r41	2011-11-02	Addressed BARB review comments, reinstated mandatory HID service discovery for Boot Mode Hosts, and optional DIS and Battery service discovery. Added optional characteristic discovery for Boot Mode hosts. Updated section 5.1.6 to refer to Scan Parameters Profile/Service. Added behavior sections for Boot mode characteristics. Added exchange MTU sub-procedure requirement for Report Hosts. Added information sharing for bonding and service changed requirement for HID Hosts.
D09r42	2011-11-08	Addressed BARB review comments. Removed optional support of Report and non-HID Service characteristic in Table 4-2.
D10r00	2011-11-23	Added clarification in Section 3.1.1 regarding external service characteristics' mandatory requirements for characteristic properties. Submitted as v1.0 voting object to BARB
D10r01	2011-12-07	Added note in Section 4.5.3 regarding multiple Battery Service instances & use of the characteristic presentation format descriptor. Resubmitted as v1.0
V10r00	2011-12-27	Adopted by the Bluetooth SIG Board of Directors

Contributors

Name	Company
Krishnan Nair	CSR
Simon Finch	CSR
Robin Heydon	CSR
Joe Decuir	CSR
Amit Gupta	CSR
Chris Church	CSR
Alain Michaud	Microsoft

Name	Company
Jacques Chassot	Logitech
David Edwin	Nordic
Sandeep Kamath	TI
Karl Torvmark	TI
Len Ott	Socket Mobile
Mike Tsai	Qualcomm Atheros
Rob Hulvey	Broadcom

Disclaimer and Copyright Notice

Document Terminology

The Bluetooth SIG has adopted Section 13.1 of the IEEE Standards Style Manual, which dictates use of the words ``shall'', ``should'', ``may'', and ``can'' in the development of documentation, as follows:

The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).

The use of the word *must* is deprecated and shall not be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

The use of the word *will* is deprecated and shall not be used when stating mandatory requirements; *will* is only used in statements of fact.

The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

Table of Contents

1 Introduction

The HID over GATT profile defines the procedures and features to be used by *Bluetooth* low energy HID Devices using GATT and *Bluetooth* HID Hosts using GATT.

This profile is an adaptation of the USB HID specification [2] to operate over a *Bluetooth* low energy wireless link.

This profile shall operate over an LE transport only. For BR/EDR, the *Bluetooth* Human Interface Device Profile Specification [9] shall be used.

1.1 Profile Dependencies

This profile requires the Generic Attribute Profile (GATT), the Battery Service, the Device Information Service, and the Scan Parameters Profile.

This specification can be used with *Bluetooth* Core Specification Version 4.0 [3] or later.

1.2 Conformance

If conformance to this profile is claimed, all capabilities indicated as mandatory for this profile shall be supported in the specified manner (process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the *Bluetooth* qualification program.

2 Configuration

2.1 Roles

This profile defines three roles: HID Device, Boot Host, and Report Host.

- The HID Device shall be a GATT server.
- The Boot Host shall be a GATT client.
- The Report Host shall be a GATT client.

Use of the term HID Host refers to both host roles: Boot Host, and Report Host. A Report Host is required to support a HID Parser and be able to handle arbitrary formats for data transfers (known as Reports) whereas a Boot Host is not required to support a HID Parser as all data transfers (Reports) for Boot Protocol Mode are of predefined length and format.

2.2 Role/Service Relationships

Figure 2.1shows the relationship between services and the profile roles.

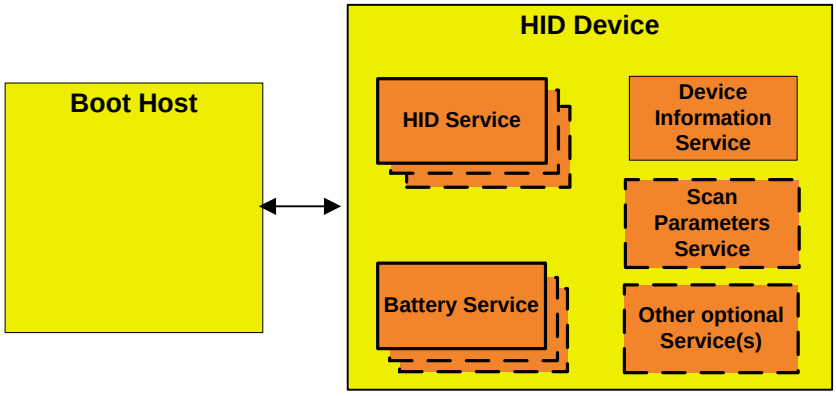

Figure 2.1: Boot Host and HID Device Roles/Service Relationship

Note: Profile roles are represented by yellow boxes and services are represented by orange boxes.

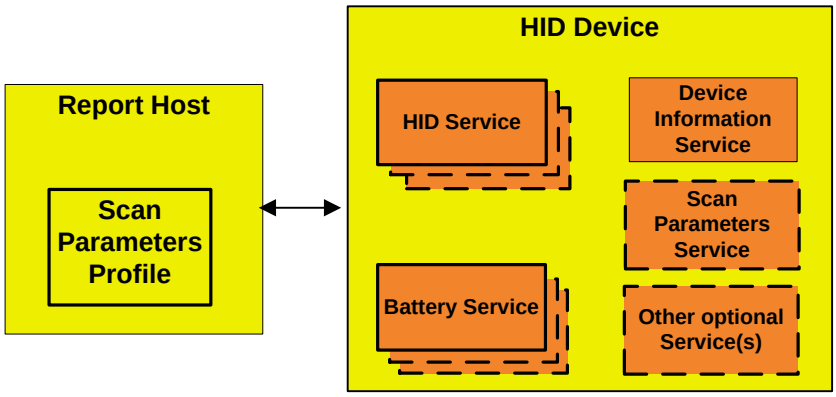

Figure 2.2: Report Host and HID Device Roles/Service Relationships

Note: Profile roles are represented by yellow boxes and services are represented by orange boxes.

The Report Host supports the Scan Client role of the Scan Parameters Profile.

The Boot Host shall not support the Scan Client role of the Scan Parameters Profile.

The HID Device has one or more instances of the HID Service, one or more instances of the Battery Service, a single instance of the Device Information Service, and optionally one instance of the Scan Parameters Service as part of Scan Server role of the Scan Parameters Profile. The HID Device may optionally have single or multiple instances of other services.

2.3 Concurrent Role Limitations and Restrictions

A Boot Host shall not concurrently be a Report Host.

A Report Host shall not concurrently be a Boot Host.

There are no concurrency limitations on either HID Host roles from also being a HID Device.

2.4 Topology Limitations and Restrictions

The HID Device shall use the GAP Peripheral role.

The Boot Host shall use the GAP Central role.

The Report Host shall use the GAP Central role.

2.5 Multiple Service Instances

Multiple service instances shall not be supported for the following services:

- Device Information Service.
- Scan Parameters Service

Multiple service instances of the HID Service may be supported to allow implementers to define composite HID Devices whose combined functions require more than 512 octets of data to describe.

- Multiple service instances of the Battery Service may be supported.
- Multiple service instances of the following may be supported, but are not considered as a part of this profile:
- Any Service other than HID Service, Device Information Service, or Scan Parameters Service.

3 HID Device Requirements

The HID Device shall have one or more instances of the HID Service, one or more instances of the Battery Service, one instance of the Device Information Service, and optionally the Scan Parameters Service, but only a single instance.

The HID Device may support the functionalities defined by the Scan Server role of the Scan Parameters Profile [7].

Table 3.1 shows service requirements for the HID Device

Service	Requirement
HID Service	M
Battery Service	M
Device Information Service	M
Scan Parameters Service	O

Table 3.1: HID Device Service Requirements

3.1 HID Service

This sub-section defines additional HID Device requirements beyond those defined in the HID Service [4].

3.1.1 Dependent Service Requirements

Any non-HID Service which has a characteristic whose value is described within the Report Map characteristic value shall be referenced as an «Include» within the HID Service definition containing that Report Map characteristic.

Any characteristic belonging to an external service whose value is described within the Report Map characteristic shall also contain a Report Reference characteristic descriptor within that external service characteristic definition. Only characteristics supporting the mandatory characteristic properties for the intended Report Type shall be described within the Report Map characteristic.

A HID Service shall not include any external service which is already included within another HID Service definition on the GATT Server. These rules prevent separate HID Services from referencing multiple characteristics of the same UUID having identical Report Reference characteristic descriptors.

3.1.2 Service Type

All services with the «HID Service» UUID shall be instantiated as a «Primary Service» as part of this profile.

3.1.3 Service UUIDs AD Type

While in a GAP Discoverable Mode for initial connection to a HID Host, the HID Device should include HID Service UUID(s) defined in [8] in the Service UUIDs AD type field of

the advertising data. Section 5.2.1 describes how a HID Host can take advantage of this feature.

3.1.4 Local Name AD Type

For enhanced user experience a HID Device should include its Local Name in its Advertising Data or Scan Response Data. Section 5.2.1 describes how a HID Host can take advantage of this feature.

3.1.5 Appearance AD Type

For enhanced user experience a HID Device should include its Appearance in its Advertising Data or Scan Response Data. Section 5.2.1 describes how a HID Host can take advantage of this feature.

3.1.6 Additional Security Requirements

This profile defines additional security requirements in Section 6.1 beyond those defined in the HID Service.

3.2 Battery Service

This sub-section defines additional HID Device requirements beyond those defined in the Battery Service [5].

3.2.1 Service Type

There shall be at least one instance of a service with the «Battery Service» UUID, instantiated as a «Primary Service». If a *Battery Level* characteristic value is described within the *Report Map* characteristic value, then the Battery Service definition in which the *Battery Level* characteristic exists shall be included, using the include definition, within the HID Service definition containing the *Report Map* characteristic.

3.2.2 Additional Security Requirements

This profile defines additional security requirements in Section 6.1 beyond those defined in the Battery Service [5].

3.3 Device Information Service

This sub-section defines additional HID Device requirements beyond those defined in the Device Information Service [6].

3.3.1 Service Type

The Device Information Service shall be instantiated as a «Primary Service» as part of this profile.

3.3.2 Mandatory Characteristics

The Device Information Service shall include the *PnP ID* characteristic for reading the PnP ID fields for the HID Device. This service is defined in the Device Information Service [6].

3.3.3 Additional Security Requirements

This profile defines additional security requirements in section 6.1 beyond those defined in the Device Information Service [6].

3.4 Scan Parameters Service

This subsection defines additional HID Device requirements beyond those defined in the Scan Parameters Service [7].

3.4.1 Additional Security Requirements

This profile defines additional security requirements in section 6.1 beyond those defined by the Scan Parameters Service [7], if implemented as part of this profile.

4 HID Host Requirements and Behaviors

The HID Host defines requirements for observing, connecting to, configuring for notification from, reading from, and writing to, a HID Device.

This section describes the procedure and characteristic requirements for a HID Host.

Procedure	Section Reference	Boot Host Requirement	Report Host Requirement
Service Discovery	4.3/4.5	M	M
- HID Service Discovery	4.3.1/4.5.1	M	M
- Device Information Service Discovery	4.3.2/4.5.2	O	M
- Battery Service Discovery	4.3.3/4.5.3	O	M
Characteristic Discovery	4.4/4.6	O	M
- HID Service Characteristic Discovery	4.6.1	O	M
- Device Information Service Characteristic Discovery	4.6.2	O	M
- Battery Service Characteristic Discovery	4.6.3	O	M
Report Map	4.7	X	M
Report	4.8	X	M
Boot Keyboard Input Report	4.4.1.2/4.12	C.2/C.3	X
Boot Keyboard Output Report	4.4.1.3/4.13	C.2/C.3	X
Boot Mouse Input Report	4.4.1.4/4.14	C.2	X
HID Information	4.10	X	M
HID Control Point	4.9	X	C.1
Protocol Mode	4.4.1/4.11	M	O
Non-HID Service characteristic defined within Report Map	4.8.1	X	M
C.1: Mandatory if the Host supports Suspend Mode, otherwise optional. C.2: Mandatory to support at least one of these features. C.3: If one of these features is supported, both features shall be supported.			

Table 4.1: Boot Host and Report Host Requirements

Requirements marked with ‘M’ are mandatory, ‘O’ are optional, and ‘X’ are excluded (not permitted).

4.1 GATT Sub-Procedure Requirements

Requirements in this section represent a minimum set of requirements for a HID Host (GATT Client). Other GATT sub-procedures may be used if supported by both GATT Client and Server.

Table 4.2 summarizes *additional* GATT sub-procedure requirements beyond those required by all GATT Clients.

GATT Sub-Procedure	Boot Host Requirement	Report Host Requirement
Discover All Primary Services	C.1	C.1
Discover Primary Services by Service UUID	C.1	C.1
Discover All Characteristics of a Service	O	C.2
Discover Characteristics by UUID	O	C.2
Discover All Characteristic Descriptors	M	M
Find included Services	X	M
Write Without Response	M	M
Write Characteristic Value	M	M
Notifications	M	M
Read using Characteristic UUID	M	M
Read Characteristic Value	M	M
Read Long Characteristic Value	X	M
Read Characteristic Descriptors	M	M
Write Characteristic Descriptors	M	M
C.1: Mandatory to support at least one of these sub-procedures. C.2: Mandatory to support at least one of these sub-procedures.		

Table 4.2: Additional GATT Sub-Procedure Requirements

Requirements marked with ‘M’ are mandatory, ‘O’ are optional, and ‘X’ are excluded (not permitted).

4.2 Scan Parameters Profile Support.

The Report Host shall support the functionality defined in the Scan Parameters Profile [7].

4.2.1 Additional Security Requirements

This profile defines additional requirements for the Scan Parameters Profile Scan Client role in section 6.2.

4.3 Service Discovery - Boot Host

The Boot Host shall perform primary service discovery using either the GATT *Discover All Primary Services* sub-procedure or the GATT *Discover Primary Services by Service UUID* sub-procedure. Fast connection parameters and procedures for connection establishment defined in section 5.2.6 are recommended to enhance Service Discovery speeds.

4.3.1 HID Service Discovery

The Boot Host shall perform primary service discovery to discover all HID Services.

4.3.2 Device Information Service Discovery

The Boot Host may perform primary service discovery to discover the Device Information Service.

4.3.3 Battery Service Discovery

The Boot Host may perform primary service discovery to discover the Battery Service.

4.4 Characteristic Discovery – Boot Host

4.4.1 HID Service Characteristic Discovery

The Boot Host may use either the GATT *Discover All Characteristics of a Service sub-procedure or the GATT Discover Characteristics by UUID sub-procedure* to discover the following characteristics for each HID Service on the GATT Server, if characteristic discovery is supported:

Protocol Mode characteristic (Section 4.4.1.1)

Boot Keyboard Input Report characteristic (section 4.4.1.2)

Boot Keyboard Output Report characteristic (section 4.4.1.3)

Boot Mouse Input Report characteristic (section 4.4.1.4)

If characteristic discovery is not supported, the Boot Host shall use the GATT *Read Using Characteristic UUID* sub-procedure to read the above HID Service characteristics for Boot Mode operation, replacing normal characteristic discovery.

4.4.1.1 Protocol Mode Characteristic

The Boot Host may discover the *Protocol Mode* characteristic for each HID Service on the GATT Server.

4.4.1.2 Boot Keyboard Input Report characteristic

The Boot Host may discover the *Boot Keyboard Input Report* characteristic for each HID Service on the GATT Server.

The Boot Host shall discover the associated *Client Characteristic Configuration Descriptor* of all *Boot Keyboard Input Report* characteristics using the GATT *Discover All Characteristic Descriptors* sub-procedure.

4.4.1.3 Boot Keyboard Output Report Characteristic

The Boot Host may discover the *Boot Keyboard Output Report* characteristic for each HID Service on the GATT Server.

4.4.1.4 Boot Mouse Input Report Characteristic

The Boot Host may discover the Boot Mouse Input Report characteristic for each HID Service on the GATT Server.

The Boot Host shall discover the associated *Client Characteristic Configuration Descriptor* of all *Boot Mouse Input Report* characteristics using the GATT *Discover All Characteristic Descriptors* sub-procedure.

4.4.2 Device Information Service Characteristic Discovery

The Boot Host may use either the GATT *Discover All Characteristics of a Service* sub-procedure or the GATT *Discover Characteristics by UUID* sub-procedure to discover the following characteristic of the Device Information Service, if characteristic discovery is supported:

PnP ID characteristic (section 4.4.2.1)

If characteristic discovery is not supported, the Boot Host may use the GATT *Read Using Characteristic UUID* sub-procedure to read the above Device Information Service characteristic, replacing normal characteristic discovery.

4.4.2.1 PnP ID Characteristic

The Boot Host may discover the *PnP ID* characteristic.

4.4.3 Battery Service Characteristic Discovery

The Boot Host may use either the GATT *Discover All Characteristics of a Service* sub-procedure or the GATT *Discover Characteristics by UUID* sub-procedure to discover the following characteristic of the Battery Service, if characteristic discovery is supported:

- *Battery Level* characteristic (section 4.4.3)

If characteristic discovery is not supported, the Boot Host may use the GATT *Read Using Characteristic UUID* sub-procedure to read the above Battery Service characteristic, replacing normal characteristic discovery.

4.4.3.1 Battery Level Characteristic

The Boot Host may discover the *Battery Level* characteristic.

4.5 Service Discovery – Report Host

The Report Host shall perform primary service discovery using either the GATT *Discover All Primary Services* sub-procedure or the GATT *Discover Primary Services by Service UUID* sub-procedure. Fast connection parameters and procedures for connection establishment defined in section 5.2.6 are recommended to enhance Service Discovery speeds.

If the Report Host supports an ATT_MTU larger than the default ATT_MTU, the Report Host shall use the GATT *Exchange MTU* sub-procedure prior to performing service discovery.

4.5.1 HID Service Discovery

The Report Host shall perform primary service discovery to discover all HID Services.

4.5.2 Device Information Service Discovery

The Report Host shall perform primary service discovery to discover the Device Information Service.

4.5.3 Battery Service Discovery

The Report Host may perform primary service discovery to discover all Battery Services.

The Report Host shall perform relationship discovery to find included services to discover all Battery Services with characteristics described within a HID Service *Report Map* characteristic value.

Note: Multiple instances of the Battery Service can be distinguished using the *Characteristic Presentation Format* characteristic descriptor of the *Battery Level* characteristic as defined by the Battery Service [5]. Within this profile, multiple *Battery Level* characteristics referenced within the *Report Map* characteristic are distinguished by the *Report Reference* characteristic descriptor.

4.6 Characteristic Discovery – Report Host

As required by GATT, the Report Host must be tolerant of additional optional characteristics of services used with this profile and used outside of this profile.

4.6.1 HID Service Characteristic Discovery

The Report Host shall use either the GATT *Discover All Characteristics of a Service* sub-procedure or the GATT *Discover Characteristics by UUID* sub-procedure to discover the characteristics of all HID services.

The Report Host shall use the GATT *Discover All Characteristic Descriptors* sub-procedure to discover the characteristic descriptors described in the following sections.

4.6.1.1 Report Map Characteristic

The Report Host shall discover all *Report Map* characteristics.

The Report Host shall discover all *External Report Reference* characteristic descriptors for each *Report Map* characteristic.

4.6.1.2 Report Characteristics

The Report Host shall discover all *Report* characteristics.

The Report Host shall discover the associated *Client Characteristic Configuration Descriptor* of all *Report* characteristics.

The Report Host shall discover the associated *Report Reference* characteristic descriptor of all *Report* characteristics.

4.6.1.3 HID Control Point Characteristic

The Report Host shall discover all *HID Control Point* characteristics, if the Report Host supports Suspend mode, to allow the Report Host to send control commands to HID Devices whenever the Report Host enters a low power Suspend Mode.

4.6.1.4 HID Information Characteristic

The Report Host shall discover all *HID Information* characteristics.

4.6.1.5 Protocol Mode Characteristic

The Report Host may discover the *Protocol Mode* characteristic for each HID Service on the GATT server.

4.6.2 Device Information Service Characteristic Discovery

The Report Host shall discover characteristics of the Device Information Service.

In order for the Report Host to discover the characteristics of the Device Information Service, it shall use either the GATT *Discover All Characteristics of a Service* sub-procedure or the GATT *Discover Characteristics by UUID* sub-procedure.

4.6.2.1 PnP ID Characteristic

The Report Host shall discover the *PnP ID* characteristic.

4.6.3 Battery Service Characteristic Discovery

The Report Host shall discover the characteristics of all Battery Services.

In order for the Report Host to discover the characteristics of all Battery Services, it shall use either the GATT *Discover All Characteristics of a Service* sub-procedure or the GATT *Discover Characteristics by UUID* sub-procedure.

4.6.3.1 Battery Level Characteristic

The Report Host shall discover all *Battery Level* characteristics to find *Battery Level* characteristics referenced within the *External Report Reference* characteristic descriptor and their associated *Report Reference* characteristic descriptors.

4.7 Report Map Behavior

The *Report Map* characteristic shall return the HID Report Descriptor when read.

The HID Report Descriptor is defined in the USB HID specification [2].

The Report Host shall read all characteristic descriptors of the *Report Map* characteristic to allow the Report Host to map information within the *Report Map* characteristic to external service characteristics used to transfer data described by the information between the Report Host and HID Device.

4.8 Report Behavior

The *Report* characteristic is used to transfer HID Service data between the Report Host and the HID Device.

The Report Host shall enable notifications, via the *Client Characteristic Configuration* descriptor, of the *Report* characteristic for all instances of the *Report* characteristic where the Report Type as defined in the *Report Reference* characteristic descriptor refers to an Input Report.

The Boot Host shall ignore notifications of the *Report* characteristic.

4.8.1 Translation Layer

Note: This profile delivers USB-IF HID data over the *Bluetooth* air interface by means of the Generic Attribute Profile [2]. If an implementation of the Report Host were to utilize a translation layer located between the GATT layer on the Report Host and the USB HID class driver, it would need to conform to the behavior described in this section.

According to sections 4.5 and 4.6, the Report Host shall perform service discovery, characteristic discovery and characteristic descriptor discovery in the specified manner.

A Report ID and a Report Type defined within the *Report Map* characteristic and referenced within *Report Reference* characteristic descriptors allows the Report Host to route GATT characteristic value data into and out of the USB HID class driver, and allows the Report Host to route USB HID class driver data into and out of GATT characteristic values.

For each separate Report ID and Report Type combination defined within the Report Map characteristic value, there shall be one of the following:

1. A HID Service Report characteristic and Report Reference characteristic descriptor within the Report characteristic definition.
2. An external service characteristic whose UUID is supplied via an External Report Reference characteristic descriptor within the Report Map characteristic definition, and whose characteristic value contains a Report Reference characteristic descriptor within the external service characteristic definition. All External Report Reference characteristic descriptors shall contain unique values within a HID Service definition.

For data transferred from the HID Device to the Report Host, the Report ID is prepended to data received by the Report Host (usually either a notification of a *Report* characteristic value, or as a read response of a *Report* characteristic value, for HID Service data) before being passed to a USB HID Class driver.

For data transferred to HID Device from Report Host, Report ID is removed from data received from a USB HID Class driver before being transmitted to the HID Device (usually a write command to a *Report* characteristic value or as a write request to a *Report* characteristic value for HID Service data).

4.9 HID Control Point Behavior

The *HID Control Point* characteristic is a control-point characteristic as defined in section 3.2.6, Part F, Volume 3 of [3]. The *HID Control Point* characteristic allows the Report Host to signal the HID Device that the Report host is entering or exiting a power saving mode known as Suspend Mode (see [9], §7.4.2).

4.10 HID Information Behavior

The *HID Information* characteristic value contains the bcdHID and bcountryCode fields as defined by the USB HID specification [2].

When a system enters a low-power Suspend Mode, the RemoteWake flag shall be used to determine whether the Report Host includes the HID Device in the set of devices that can wake it up.

If the RemoteWake flag is FALSE, then the HID device does not consider itself remote wakeup-capable, and the Report Host can exclude the HID Device from the set of devices that can wake the Report Host up.

When a Report Host is exiting a low power Suspend Mode, the NormallyConnectable flag shall be used to determine whether the Report Host can connect to the HID Device before any user interaction occurs on the HID device. This may be used to improve the perceived responsiveness of the system.

4.11 Protocol Mode Behavior

The *Protocol Mode* characteristic allows reading and writing of the protocol mode of the HID Service, and to set the desired protocol mode.

The Boot Host shall write to the *Protocol Mode* characteristic for each HID Service on the GATT Server, and set the characteristic value to the defined value for Boot Protocol Mode following connection establishment. There are no requirements on a Report Host to use the *Protocol Mode* characteristic.

4.12 Boot Keyboard Input Report Behavior

The *Boot Keyboard Input Report* characteristic is used to transfer HID Service data representing keyboard keystrokes between a HID Service corresponding to a HID Device operating in Boot Protocol Mode as a keyboard and a Boot Host.

If the Boot Host supports the *Boot Keyboard Input Report* characteristic, it shall enable notifications of the Boot *Keyboard Input Report* characteristic using the *Client Characteristic Configuration* descriptor.

The Report Host shall ignore notifications of the *Boot Keyboard Input Report* characteristic.

4.13 Boot Keyboard Output Report Behavior

The *Boot Keyboard Output Report* characteristic is used to transfer HID Service data representing the status of LED’s visible to the user between a HID Service

corresponding to a HID Device operating in Boot Protocol Mode as a keyboard and a Boot Host.

4.14 Boot Mouse Input Report Behavior

The *Boot Mouse Input Report* characteristic is used to transfer HID Service data representing pointer coordinates between a HID Service corresponding to a HID Device operating in Boot Protocol Mode as a mouse and a Boot Host.

If the Boot Host supports the *Boot Mouse Input Report* characteristic it shall enable notifications of the *Boot Mouse Input Report* characteristic using the Client Characteristic Configuration descriptor.

The Report Host shall ignore notifications of the *Boot Mouse Input Report* characteristic.

4.15 Battery Level Behavior

The *Battery Level* characteristic may either be read by the HID Host, or be enabled for notification using the *Client Characteristic Configuration Descriptor*, by the HID Host. The HID Host should minimize the frequency of reads of the *Battery Level* characteristic value to avoid significant impact on the battery life of the HID Device. The HID Host may use the information returned in a read response or a notification of the *Battery Level* characteristic value to display the battery level of the HID Device.

4.16 PnP ID Behavior

The *PnP ID* characteristic value shall be read by the Report Host upon initial connection establishment and may be cached afterwards. The *PnP ID* characteristic value may be read by the Boot Host upon initial connection establishment and may be cached afterwards.

The HID Host can use the information returned in the *PnP ID* characteristic value to find representative icons or load associated support software.

Note: The Appearance AD type (see section 5.2.1) exists and may be common to multiple distinct devices, however icons unique to a single manufacturer, based on the PnP ID characteristic value, can be displayed on a per-device basis.

4.17 Information Sharing between HID Hosts

The Boot Host and Report Host shall share bonding information and information regarding «Service changed» indications. If a bond is deleted from a Report Host, the bonding information shall be removed from the Boot Host. If a bond is deleted from a Boot Host, the bonding information shall be removed from the Report Host.

If a «Service changed» indication is received by the Report Mode Host when connected to the HID Device, the Report Host shall make the Boot Host aware of the «Service changed» indication and any information contained therein. If a «Service changed» indication is received by the Boot mode Host when connected to the HID Device, the Boot mode host shall make the Report mode Host aware of the «Service changed» indication and any information contained therein.

5 Connection Establishment

This section describes the connection establishment and connection termination procedures used by a HID Host and HID Device in certain scenarios.

5.1 HID Device Requirements

5.1.1 Device Discovery

The HID Device should use the GAP *Limited Discoverable Mode* when establishing an initial connection. The T_{GAP}(lim_adv_timeout) used during GAP *Limited Discoverable Mode* may be larger than the value specified in [3], Section 16, Appendix A in the GAP specification but the value shall be less than or equal to 180 seconds.

5.1.2 Connection Procedure for Non-bonded Devices

This procedure is used for connection establishment when the HID Device connects to a HID Host to which it is not bonded. This may be initiated through user interaction.

It is recommended that the HID Device advertises using the parameters in Table 5.1. The interval values in the first row are designed to attempt fast connection during 180 seconds.

Advertising Duration	Parameter	Value
180 seconds (fast connection)	Advertising Interval	30 ms to 50 ms

Table 5.1: Recommended Advertising Parameters for Non-bonded Devices

The advertising interval and time to perform advertising should be configured with consideration for user expectations of connection establishment time.

The HID Device shall accept any valid values for connection interval and connection latency set by the HID Host, as a fast connection interval may be requested in order for the HID Host to quickly perform service discovery and enable encryption.

After service discovery and encryption, the HID Device should request to change to the preferred connection parameters that best suit its use case.

To request a change in the connection parameters, the HID Device shall use the L2CAP Connection Parameter Update Request as described in [Vol.3] Part A, Section 4.20 of [3].

If the HID Host receives the L2CAP Connection Parameter Update request but has not yet completed service discovery or has not completed encryption, the HID Host may send the L2CAP Connection Parameter Update Response with the *Result* field indicating that the request has been rejected. In this case, the HID Device may wait and re-send a new L2CAP Connection Parameter Update Request no sooner than T_{GAP}(conn_param_timeout) (see [3] Volume 3, Part C, Section 9.3.9.2) seconds later.

If a connection is not established within a time limit defined by the HID Device, the HID Device may exit the GAP connectable mode.

The HID Device shall be in a bondable mode during this procedure to optimize connecting to the HID Host, again using the procedure described in Section 5.1.3 and section 5.1.4.

If a bond is created, the HID Device should write the address of the HID Host in the HID Device controller's white list and set the HID Device controller's advertising filter policy to 'process scan and connection requests only from devices in the White List'.

Once connected, the HID Device should wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to complete configuration.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications but the HID Device has no data to transfer, the HID Device should wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to terminate the connection once its actions are complete.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications and the HID Device has data to transfer, after it has completed its transfer, it should perform the GAP *Terminate Connection* procedure after waiting for an idle connection timeout.

5.1.3 Device-Initiated Connection Procedure for Bonded Devices

This procedure is used after the HID Device has bonded with the Host using the connection procedure in section 5.1.2. The HID Device may initiate the connection procedure when commanded by the user or autonomously when a notification is pending.

A HID Device shall enter the GAP Undirected Connectable Mode or Directed Connectable Mode either when commanded by the user to initiate a connection to a HID Host or when the HID Device has one or more notifications to send to a previously connected HID Host.

The HID Device when bonded should use whichever advertising filter policy it has previously configured when using the connection procedure in section 5.1.2.

The HID Device should use the recommended advertising interval values shown in Table 5.2. The interval values in the first row are designed to attempt fast connection during the first 1.28 seconds; however, if a connection is not established within that time, the interval values in the second row are designed to reduce power consumption for devices that continue to advertise.

Advertising Duration	Parameter	Value
1.28 seconds (low latency) – Option 1	Advertising mode	Directed
30 seconds (higher latency) - Option 2	Advertising mode	Undirected
	Advertising Interval	20 ms to 30 ms

Table 5.2: Recommended advertising parameters for device-initiated connection of bonded devices

The advertising interval and time to perform advertising should be configured with consideration for user expectations of connection establishment time.

The HID Device shall accept any valid values for connection interval and connection latency set by the HID Host until service discovery, bonding and/or encryption is

complete. Only after that should the HID Device request to change to its preferred connection parameters which best suit its use case.

If a connection is not established within a time limit defined by the HID Device, the HID Device may exit the GAP connectable mode or switch to the Advertising parameters shown in Table 5.2 if NormallyConnectable is TRUE.

When a connection is established with a notification pending, the HID Device shall send one or more notifications to the HID Host.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications but the HID Device has no data to transfer, it should wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to terminate the connection once its actions are complete.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications and the HID Device has data to transfer, after it has completed its transfer, it should perform the GAP *Terminate Connection* procedure after waiting for an idle connection timeout.

Refer to Appendix A for details on NormallyConnectable behavior.

5.1.4 Host-Initiated Connection Procedure for Bonded Devices

This procedure is used after the HID Device has bonded with the HID Host using the connection procedure in section 5.1.2. The HID Host may initiate the connection procedure when commanded by the user or autonomously when data such as LED status needs to be transmitted to the HID Device.

A HID Device that wishes to be able to accept connections initiated by bonded Report Hosts shall set the NormallyConnectable flag to TRUE in the *HID Information* characteristic. When NormallyConnectable is TRUE, a HID Device bonded to at least one Report Host shall be in the GAP Undirected Connectable Mode whenever it is not connected to any HID Host.

The HID Device when bonded should use whichever advertising filter policy it has previously configured when using the connection procedure in section 5.1.2.

The HID Device should use the recommended advertising interval values shown in Table 5.3.

Advertising Duration	Parameter	Value
Permanent (reduced power)	Advertising mode	Undirected
	Advertising Interval	1 s to 2.5 s

Table 5.3: Recommended Advertising Parameters for Host-Initiated Connection of Bonded Devices

The advertising interval and time to perform advertising should be configured with consideration for user expectations of connection establishment time.

The HID Device shall accept any valid values for connection interval and connection latency set by the HID Host until service discovery, bonding and encryption is complete. Only after that should the HID Device request to change to its preferred connection parameters which best suit its use case.

When a connection is established with a notification pending, the HID Device shall send one or more notifications to the HID Host.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications but the HID Device has no data to transfer, it should wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to terminate the connection once its actions are complete.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications and the HID Device has data to transfer, after it has completed its transfer, it should perform the GAP *Terminate Connection* procedure after waiting for an idle connection timeout.

Refer to Appendix A for details on NormallyConnectable behavior.

5.1.5 Link Loss Reconnection Procedure

When a connection is terminated due to link loss a HID Device should attempt to reconnect to the HID Host by entering a GAP connectable mode using the recommended advertising interval values shown in Table 5.2. The HID Device may also wait until it has data to transmit or until the next user activity is detected.

5.1.6 Idle Connection

The HID Device may perform the GAP *Terminate Connection* procedure if the connection is idle for a time period, which is implementation specific. If the HID Device supports the Scan Parameters Service, the Report Host shall follow the procedures defined in the *Scan Parameters Profile* to write its intended scanning behavior to the *Scan Interval Window* characteristic, and should not terminate the connection, but should wait for the HID Device to terminate the connection.

The HID Device may use the scan parameters written to the *Scan Interval Window* characteristic by the Report Host when deciding whether to remain connected to the Report Host or to terminate the connection, depending on the power consumption or reconnection latency requirements of the HID Device.

5.2 Host Requirements

5.2.1 Device Discovery

The HID Host should use the GAP *Limited Discovery Procedure* to discover HID Devices.

The HID Host may identify devices based on their Service UUIDs AD Type data and display devices supporting HID Services to the user before initiating a connection. The HID Host may also identify devices based on their Local Name AD Type data to provide a meaningful name for the device. The HID Host may also identify devices based on their Appearance AD Type data to display meaningful icons for the device.

5.2.2 Connection Procedure for Non-bonded Devices

This procedure is used for connection establishment when the HID Host connects to a HID Device to which it is not bonded. This may be initiated through user intervention.

A HID Host may use one of the following GAP connection procedures defined in [3], Volume 3, Part C, §9.3, based on its connectivity requirements:

1. *General Connection Establishment Procedure*. The HID Host may use this procedure when it requires connection to one or more HID Devices. This procedure allows a HID Host to connect to a HID Device discovered during a scan without using the white list.
2. *Direct Connection Establishment Procedure*. The HID Host may use this procedure when it requires connection to a single HID Device.
3. *Auto Connection Establishment Procedure*. The HID Host may use this procedure when it requires connecting to one or more HID Devices. This procedure will automatically connect to a HID Device in the white list.
4. *Selective Connection Establishment Procedure*. The HID Host may use this procedure when it requires connecting to one or more HID Devices. This procedure allows a HID Host to connect to a HID Device discovered during a scan while using the white list.

The HID Host should use the recommended Scan Interval and Scan Window values shown in Table 5.4.

For 180 seconds (or optionally continuously for mains powered devices), the HID Host should use the recommended Scan Window / Scan Interval pair to attempt fast connection.

Scan Duration	Parameter	Value
180 seconds (fast connection)	Scan Interval	22.5ms
	Scan Window	11.25ms

Table 5.4: Recommended Scan Parameters for Non-bonded Devices

The HID Host shall bond with the HID Device during this procedure to optimize reconnecting to the HID Device using the procedure in section 5.2.3 and section 5.2.4.

If a bond is created, the HID Host should write the address of the HID Device in the HID Host controller's white list and set the HID Host controller's initiator filter policy to 'process connectable advertisement packets'.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications, the HID Host should wait for an idle connection timeout (refer to section 5.1.6) before terminating the connection in case the HID Device has any notifications pending.

The HID Device typically terminates the connection after completion of data transfer, but may wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to terminate the connection once its actions are complete.

5.2.3 Device-Initiated Connection Procedure for Bonded Devices

This procedure is used after the HID Host has bonded with the HID Device using the connection procedure in section 5.2.2.

The HID Device may initiate the connection procedure either when commanded by the user or autonomously when a notification is pending.

A HID Host may use one of the GAP connection procedures (see section 5.2.2) based on its connectivity requirements.

The HID Host should use the scan interval and scan window values shown in Table 5.5. Scan intervals greater than 1.28 s and scan windows shorter than 11.25 ms should not be used.

Scan Duration	Parameter	Value
Permanent (reduced power)	Scan Interval	1.28s
	Scan Window	11.25ms

Table 5.5: Recommended Scan Parameters for Device-Initiated Connection of Bonded Devices

The HID Host should use a scan window and scan interval suitable to its power and connection time requirements. Increasing the scan window increases the power consumption, but decreases the connection time.

The scan interval and scan window should be configured with consideration for user expectations of connection establishment time.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications, the HID Host should wait for an idle connection timeout (see section 5.1.6) before terminating the connection in case the HID Device has any notifications pending.

The HID Device typically terminates the connection after completion of data transfer, but may wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to terminate the connection once its actions are complete.

The HID Host shall start encryption after connection establishment to verify the status of the bond.

If encryption fails upon connection establishment (i.e., the bond no longer exists), the HID Host must, after user interaction, perform bonding, perform service discovery (unless the HID Host had previously determined that the HID Device did not have the «Service Changed» characteristic), and reconfigure the HID Device *Client Characteristic Configuration* descriptor before using any of the this profile's services in case the previous configuration was altered or lost.

5.2.4 Host-Initiated Connection Procedure for Bonded Devices

This procedure is used after the HID Host has bonded with the HID Device using the connection procedure in section 5.2.2.

The HID Host may initiate the connection procedure when commanded by the user or autonomously when data such as LED status needs to be transmitted to the HID Device.

Note: The Report Host should only attempt to connect to a bonded HID Device if the HID Device has the NormallyConnectable flag set to TRUE.

A HID Host may use one of the connection procedures (see section 5.2.2) based on its connectivity requirements.

The HID Host should use the recommended scan interval and scan window values shown in Table 5.6.

Scan Duration	Parameter	Value
30 seconds (fast connection)	Scan Interval	30ms to 60ms*
	Scan Window	30ms

Table 5.6: Recommended Scan Parameters for Host-Initiated Connection of Bonded Devices

* A scan interval of 60ms is recommended when the HID Host is supporting other operations to provide a 50% scan duty cycle versus 100% scan duty cycle.

If a connection is not established within that time, the HID Host may exit the GAP connection procedure.

The HID Host should use a scan window and scan interval suitable to its power and connection time requirements. Increasing the scan window increases the power consumption, but decreases the connection time.

The scan interval and scan window should be configured with consideration for user expectations of connection establishment time.

If the *Client Characteristic Configuration* descriptor has been configured to enable notifications, the Host should wait for an idle connection timeout (refer to section 5.1.6) before terminating the connection in case the HID Device has any notifications pending.

The HID Device typically terminates the connection after completion of data transfer, but may wait for an idle connection timeout (refer to section 5.1.6) to allow the HID Host to terminate the connection once its actions are complete.

The HID Host shall start encryption after connection establishment to verify the status of the bond.

If encryption fails upon connection establishment (i.e. the bond no longer exists), the HID Host must, after user interaction, perform bonding, perform service discovery (unless the Host had previously determined that the HID Device did not have the «Service Changed» characteristic), and configure the HID Device *Client Characteristic Configuration* descriptor again before using any of the services referenced by this profile in case the configuration was altered or lost.

Refer to Appendix A for details on NormallyConnectable behavior.

5.2.5 Link Loss Reconnection Procedure

When a connection is terminated due to link loss, the HID Host should attempt to reconnect to the HID Device using any of the GAP connection procedures (see section 5.2.2). The Report Host should use the parameters in Table 5.6 if the HID Device has set the NormallyConnectable flag to TRUE.

5.2.6 Fast Connection Interval

To avoid very long service discovery and encryption times, the HID Host should use the connection intervals defined in Table 5.7 in the connection request.

Parameter	Value
Minimum Connection Interval	7.5 ms
Maximum Connection Interval	50 ms

Table 5.7: Recommended Fast Connection Parameters

If, at any time, lower latency is required, for example to perform encryption key refresh or encryption setup, this should be preceded with a connection parameter update to the minimum and maximum connection interval values defined in Table 5.7 and a slave latency value of zero. This fast connection interval should be maintained as long as lower latency is required. Afterwards, the connection parameters should return to those specified by the HID Device using the L2CAP Connection Parameter Update procedure.

6 Security Considerations

This section describes the security considerations for a HID Device and HID Host.

6.1 Device Security Considerations

The HID Device shall use LE Security Mode 1 and either Security Level 2 or 3.

All supported characteristics specified by the HID Service shall be set to Security Mode 1 and either Security Level 2 or 3.

HID Devices shall bond and use LE Security Mode 1, Security Level 2 or 3, both of which require an encrypted link. Encryption is used to verify that a bond still exists and is valid.

The HID Device should use the SM Slave Security Request, as defined in [3] Volume 3, Part H, Section 2.4.6, procedure to inform the HID Host of its security requirements.

All supported characteristics specified by the Device Information Service, Scan Parameters Service and Battery Service should be set to the same LE Security Mode and the same Security Level as the characteristics in the HID Service.

6.2 Host Security Considerations

The HID Host shall bond with the HID Device.

The HID Host shall support LE Security Mode 1 and Security Level 2 and optionally Security Level 3.

The HID Host shall accept any valid LE Security Mode and Security Level combination requested by the HID Device.

The HID Host shall only initiate an encryption key refresh on receipt of a SM Slave Security Request, as defined in [3] Volume 3, Part H, Section 2.4.6, from the HID Device.

7 List of Figures

8 List of Tables

9 Acronyms and Abbreviations

Acronyms and Abbreviations	Meaning
AD	Advertising Data
BR/EDR	Basic Rate / Enhanced Data Rate
GAP	Generic Access Profile
GATT	Generic Attribute Profile
HID	Human Interface Device
LE	Low Energy
SM	Security Manager
UUID	Universally Unique Identifier
USB	Universal Serial Bus

Table 9.1: Acronyms and Abbreviations

10 References

[1] USB HID Usage Tables, Version 1.12 (www.usb.org)
[2] USB Device Class Definition for Human Interface Devices (USB HID Specification), Version 1.11 (www.usb.org)
[3] *Bluetooth* Core Specification version 4.0 or later
[4] HID Service v1.0
[5] Battery Service v1.0
[6] Device Information Service v1.0
[7] Scan Parameters Profile v1.0
[8] Characteristic and Descriptor descriptions are accessible via the Bluetooth SIG Assigned Numbers.
[9] *Bluetooth* HID Profile Specification v1.0

11 Appendix A

Table 11.1 details the Host and Device connection behavior as a function of NormallyConnectable bit of the HID Information characteristic.

Normally Connectable		**LE reconnection requirements**	**Comments**
FALSE		Device: - if data to transmit: high duty-cycle advertising for 5s - if idle: radio off Host: - low duty-cycle scanning	Most common configuration
TRUE		Device: - if data to transmit: high duty-cycle advertising for 5s - if idle: low duty-cycle advertising Host: - if data to transmit: high duty-cycle scanning for 5s - if idle: low duty-cycle scanning	In this case, it is preferred to keep the LE HID connection active always.

Table 11.1: HID Host and HID Device Connection Behavior