Ranging Profile

***Bluetooth*® Profile Specification**

- **Version:** v1.0
- **Version Date:** 2024-11-12
- **Prepared By:** Direction Finding Working Group

Abstract:

The Ranging Profile (RAP) specification allows a distance-measurement application to read ranging results from a remote device and configure the desired content and delivery method.

Version History

Version Number	Date (yyyy-mm-dd)	Comments
v1.0	2024-11-12	Adopted by the Bluetooth SIG Board of Directors.

Acknowledgments

Name	Company
Hai Shalom	Google LLC
Pouria Zand	Infineon Technologies AG
Kim Schulz	Samsung Electronics Co., Ltd.
Mayank Batra	Qualcomm Technologies, Inc.
Josselin de la Broise	Tile, Inc.
Khaled Elsayed	Synopsys, Inc.
Ealwan Lee	SKAIChips Co., Ltd.
Jonathan Berner	E.G.O. Elektro-Gerätebau GmbH
Arne Bestmann	Lambda:4 Entwicklungen GmbH
Jere Knaappila	Silicon Laboratories
Piotr Pryga	Nordic Semiconductor ASA
Victor Zhodzishsky	Infineon Technologies AG
Robert Hughes	Intel Corporation
Mohamed Ratni	Sony Group Corporation
Kyle Golsch	Denso Corporation
Robert Hulvey	Meta Platforms, Inc.
Daniela Dumitrache	NXP B.V.
Jan Slupski	Telink Semiconductor (Shanghai) Co., Ltd

Contents

1 Introduction 6

1.1 Language 6

1.1.1 Language conventions 6

1.1.1.1 Implementation alternatives 6

1.1.1.2 Discrepancies 6

1.1.2 Reserved for Future Use 7

1.1.3 Prohibited 7

1.2 Table requirements 7

1.3 Conformance 7

2 Configuration 8

2.1 Roles 8

2.2 Role and service relationships 8

2.3 Concurrency limitations and restrictions 8

2.4 Topology limitations and restrictions 8

2.5 Bluetooth specification release compatibility 9

2.6 Transport dependencies 9

3 RRSP role requirements 10

3.1 RRSP requirements 10

3.1.1 Advertising Data 10

3.1.2 Maximum transmission unit 10

3.2 Additional Ranging Service requirements 10

3.2.1 Ranging Data retention requirements 10

4 RREQ role requirements 12

4.1 Maximum transmission unit 12

4.2 CS security and accuracy levels 12

4.3 Service discovery 13

4.3.1 Characteristic discovery 13

4.3.2 RAS Features characteristic 13

4.4 Ranging Data characteristics 13

4.4.1 Real-time Ranging Data characteristic 13

4.4.1.1 Real-time Ranging Data notification or indication timeouts 14

4.4.2 On-demand Ranging Data characteristic 15

4.4.2.1 Retransmission of lost Ranging Data segments 16

4.4.3 Ranging Data Ready characteristic 17

4.4.3.1 Ranging Data Ready timeout 18

4.4.4 Ranging Data Overwritten characteristic 18

4.4.5 Ranging Data segments received out of order 19

4.5 RAS Control Point characteristic 19

4.5.1 RAS Control Point characteristic write operations 19

4.5.1.1 Configuration of the Ranging Data Filter 20

4.5.1.2 Abort Operation 20

4.5.2 RAS Control Point characteristic indications 20

4.5.2.1 RAS Control Point Complete Ranging Data Response 20

4.5.2.2 RAS Control Point Complete Lost Ranging Data Segment Response 20

4.5.3 RAS Control Point Response 21
4.5.4 RAS Control Point procedure error and timeout handling 21
4.5.4.1 On-demand Ranging Data notification or indication timeouts 21
4.5.4.2 RAS Control Point indications error handling 21
4.6 Summary of GATT sub-procedures for RREQ 21
5 Connection establishment procedures 23
6 Security requirements 24
6.1 Bluetooth device address requirements 24
6.2 General security requirements 24
6.3 Out-of-band pairing 24
6.4 Security requirements for BR/EDR 25
7 Additional requirements for BR/EDR 26
8 Acronyms and abbreviations 27
9 References 28

1 Introduction

The Ranging Profile (RAP) specification can be used by a distance-measurement application on a device to read remote ranging results of an ongoing Channel Sounding (CS) procedure and configure the desired content and delivery method from a remote device.

Examples of distance-measurement applications include car and door locks that implement seamless unlocking and locking, as a person using a handheld mobile device approaches or departs the lock. Other uses include asset tracking in a warehouse and smart functionality based on proximity.

1.1 Language

1.1.1 Language conventions

In the development of a specification, the Bluetooth SIG has established the following conventions for use of the terms *"shall"*, *"shall not"*, *"should"*, *"should not"*, *"may"*, *"must"*, and *"can"*. In this Bluetooth specification, the terms in Table 1.1 have the specific meanings given in that table, irrespective of other meanings that exist.

Term	Definition
shall	—used to express what is required by the specification and is to be implemented exactly as written without deviation
shall not	—used to express what is forbidden by the specification
should	—used to express what is recommended by the specification without forbidding anything
should not	—used to indicate that something is discouraged but not forbidden by the specification
may	—used to indicate something that is permissible within the limits of the specification
must	—used to indicate either: 1. an indisputable statement of fact that is always true regardless of the circumstances 2. an implication or natural consequence if a separately-stated requirement is followed
can	—used to express a statement of possibility or capability

Table 1.1: Language conventions terms and definitions

1.1.1.1 Implementation alternatives

When specification content indicates that there are multiple alternatives to satisfy specification requirements, if one alternative is explained or illustrated in an example it is not intended to limit other alternatives that the specification requirements permit.

1.1.1.2 Discrepancies

It is the goal of Bluetooth SIG that specifications are clear, unambiguous, and do not contain discrepancies. However, members can report any perceived discrepancy by filing an erratum and can request a test case waiver as appropriate.

1.1.2 Reserved for Future Use

Where a field in a packet, Protocol Data Unit (PDU), or other data structure is described as "Reserved for Future Use" (irrespective of whether in uppercase or lowercase), the device creating the structure shall set its value to zero unless otherwise specified. Any device receiving or interpreting the structure shall ignore that field; in particular, it shall not reject the structure because of the value of the field.

Where a field, parameter, or other variable object can take a range of values, and some values are described as "Reserved for Future Use," a device sending the object shall not set the object to those values. A device receiving an object with such a value should reject it, and any data structure containing it, as being erroneous; however, this does not apply in a context where the object is described as being ignored or it is specified to ignore unrecognized values.

When a field value is a bit field, unassigned bits can be marked as Reserved for Future Use and shall be set to 0. Implementations that receive a message that contains a Reserved for Future Use bit that is set to 1 shall process the message as if that bit was set to 0, except where specified otherwise.

The acronym RFU is equivalent to Reserved for Future Use.

1.1.3 Prohibited

When a field value is an enumeration, unassigned values can be marked as “Prohibited.” These values shall never be used by an implementation, and any message received that includes a Prohibited value shall be ignored and shall not be processed and shall not be responded to.

Where a field, parameter, or other variable object can take a range of values, and some values are described as “Prohibited,” devices shall not set the object to any of those Prohibited values. A device receiving an object with such a value should reject it, and any data structure containing it, as being erroneous.

“Prohibited” is never abbreviated.

1.2 Table requirements

Requirements in this specification are defined as "Mandatory" (M), "Optional" (O), "Excluded" (X), “Not Applicable” (N/A), or "Conditional" (C.n). Conditional statements (C.n) are listed directly below the table in which they appear.

1.3 Conformance

Each capability of this specification shall be supported in the specified manner. This specification may provide options for design flexibility, because, for example, some products do not implement every portion of the specification. For each implementation option that is supported, it shall be supported as specified.

2 Configuration

2.1 Roles

RAP defines two roles:

- Ranging Responder (RRSP): A device that makes ranging results available to a remote device by implementing the Ranging Service (RAS) [2].
- Ranging Requester (RREQ): A device that requests ranging results from an RRSP by acting as a client to RAS on the RRSP. The RREQ is implemented on a device which also contains a distance-measurement application that uses the RREQ to request the ranging results, and which then processes the results to produce distance estimations.

2.2 Role and service relationships

The following profile role and service relationships apply:

- The RRSP shall be a Generic Attribute Profile (GATT) Server that implements the RAS Server and may support the establishment of an Enhanced Attribute Profile (EATT) bearer.
- The RREQ shall be a GATT Client and may support the establishment of an EATT bearer.

2.3 Concurrency limitations and restrictions

No concurrency limitations or restrictions are imposed by RAP. A device may implement the RREQ or the RRSP at the same time and together with other profiles.

2.4 Topology limitations and restrictions

Because there are no topology restrictions imposed by this profile, the RREQ and the RRSP shall have either the Generic Access Profile (GAP) Central or Peripheral roles (see Volume 3, Part C, Section 2.2.2 in [1]).

The RREQ and the RRSP shall have either the CS Initiator or Reflector roles in the Core Controller.

Figure 2.1 shows the relationship between RAS and the two RAP roles.

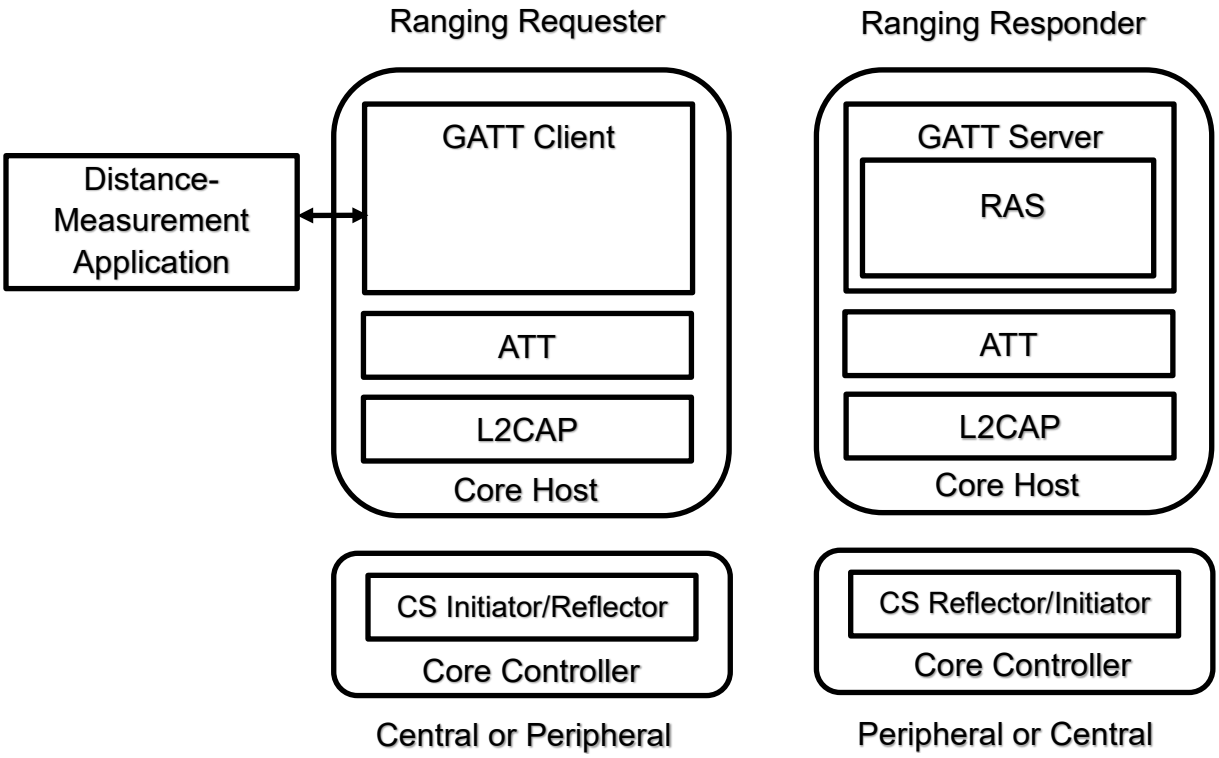

Figure 2.1: High-level architecture of RAP and RAS

2.5 Bluetooth specification release compatibility

This specification is compatible with Bluetooth Core Specification Version 6.0 or later [1].

2.6 Transport dependencies

RAP is specified only for operation over the Bluetooth Low Energy (LE) transport.

3 RRSP role requirements

This section describes the profile role requirements for an RRSP.

The RRSP shall instantiate at least one instance of RAS. RAS shall be instantiated as a «Primary Service».

Table 3.1 shows the service requirements for the RRSP role.

Service	Support in RRSP	Section for Additional Requirements
Ranging Service	M	3.2

Table 3.1: Requirements for the RRSP

3.1 RRSP requirements

This section describes RRSP role requirements in addition to the RAS Server requirements defined in RAS.

3.1.1 Advertising Data

If the RRSP is a device that implements the Peripheral role of GAP (see Volume 3, Part C, Section 2.2 in [1]), then while the RRSP is in a GAP General or Limited Discoverable mode for initial connection to an RREQ, the RRSP should include the «Ranging Service UUID», as defined in [3] in the Service Universally Unique Identifiers (UUIDs) AD Type field of the Advertising Data (AD).

3.1.2 Maximum transmission unit

The RRSP should support a Maximum Transmission Unit (MTU) size of at least 247 octets to allow faster data transfer and lower latency, reduce the number of segments in each CS Procedure, and reduce the overhead for each segment. The Ranging Data size may be in the range of 1.5 KB and 5.5 KB. Devices that use the default Bluetooth LE ATT_MTU size of 23 octets (see Volume 3, Part G, Section 5.2.1 in [1]) will require approximately 75 to 275 segments accordingly to transfer the Ranging Data.

If the RRSP operates on top of EATT, then the ATT_MTU that is used by the RRSP shall be the ATT_MTU value used by the bearer with the minimum ATT_MTU value (see Volume 3, Part G, Section 4.3.1 in [1]).

3.2 Additional Ranging Service requirements

3.2.1 Ranging Data retention requirements

Ranging Data retention requirements are specified in Section 2.7.2.1 in [2]. In addition, the RRSP shall retain the most recent Ranging Data for each connected RREQ until one of the following conditions is met:

- The RRSP is configured to notify or indicate Real-time Ranging Data and the Ranging Data was notified or indicated to the RREQ.
- The RREQ writes the ACK_Ranging_Data command to the RAS Control Point after the RRSP notified or indicated all On-demand data and sent the Complete Ranging Data indication.

- New CS Procedure Ranging Data is available and the RRSP does not have enough memory to retain additional Ranging Data.
- A maximum timeout of 10 seconds, or a shorter implementation configurable timeout value, has elapsed since the RRSP indicated a Complete Ranging Data indication and the RREQ did not respond with an ACK_Ranging_Data command or a Retrieve_Lost_Ranging_Data command.

If the RRSP queues more than one CS Procedure Data and does not have enough memory to retain an incoming CS Procedure Data, then the RRSP shall delete the oldest CS Procedure Data in its queue and shall follow the Ranging Data Overwritten indication or notification as specified in Section 2.7.2.2 in [2].

The Ranging Data retention requirements shall apply for every connected RREQ.

4 RREQ role requirements

Table 4.1 describes the procedure requirements for the RREQ.

Requirement	Support in RREQ	Section
Service discovery for RAS	M	4.3
Characteristic discovery	M	4.3.1
Sub-procedure requirements	M	4.6
RAS Features characteristic	M	4.3.2
Real-time Ranging Data characteristic	O	4.4.1
On-demand Ranging Data characteristic	M	4.4.2
RAS Control Point characteristic	M	4.5
Ranging Data Ready characteristic	M	4.4.3
Ranging Data Overwritten characteristic	M	4.4.4

Table 4.1: Procedure requirements for the RREQ

4.1 Maximum transmission unit

The RREQ should support an MTU size of at least 247 octets to allow faster data transfer and lower latency, reduce the number of segments in each CS Procedure, and reduce the overhead for each segment.

The Ranging Data size may be in the range of 1.5 KB and 5.5 KB. Devices that use the default Bluetooth LE ATT_MTU size of 23 octets (see Volume 3, Part G, Section 5.2.1 in [1]) will require approximately 75 to 275 segments accordingly to transfer the Ranging Data. Therefore, the RREQ should initiate an update of the ATT_MTU value (see Volume 3, Part G, Section 4.3.1 in [1] for the Unenhanced Attribute Profile (ATT) bearer, and Volume 3, Part G, Section 5.3.1 in [1] for EATT). If the Ranging Data is segmented to more than 64 segments, then the RREQ does not have a way to retrieve a lost segment with a higher index value of 63.

4.2 CS security and accuracy levels

There are four CS security and accuracy levels defined in Volume 3, Part C, Section 10.11.1 in [1].

A distance-measurement application on the RREQ should query the local and remote Core Controller capabilities that are exchanged during the Link Layer (LL) capabilities exchange before initiating a CS Procedure (see Volume 6, Part B, Section 2.4.2.44 in [1]) to determine if the local and remote Core Controller capabilities meet its minimum CS security and accuracy requirements. If the security and accuracy requirements are not met, then the distance-measurement application on the RREQ should terminate the Asynchronous Connection-oriented logical transport (ACL) connection and may inform the user, if applicable.

In addition, a distance-measurement application on the RREQ should set the highest CS security and accuracy level supported by both sides, but the distance-measurement application may set a lower level based on its needs and constraints via the Core Controller-level CS Procedure setup and configuration process.

4.3 Service discovery

When the RREQ is performing primary service discovery, the RREQ shall use either the GATT Discover All Primary Services sub-procedure or the GATT Discover Primary Services by Service UUID sub-procedure.

The RREQ shall discover RAS on the RRSP.

The procedures in Section 4.3.1 shall be used to discover characteristics for use with RAP.

4.3.1 Characteristic discovery

The RREQ shall be tolerant of additional optional or vendor-specific characteristics in the service records of services used with RAP.

The RREQ 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 the service.

The RREQ shall use the GATT Discover All Characteristic Descriptors sub-procedure to discover any required characteristic descriptors.

4.3.2 RAS Features characteristic

The RREQ shall obtain information about the capabilities of the Ranging operations supported by the RRSP by reading the value of the RAS Features characteristic. The RREQ shall parse the information to determine the features supported by RAS (as described in [2]) and adjust its RAS operation configuration accordingly to be compatible with the capabilities supported by the RRSP.

4.4 Ranging Data characteristics

RAS in the RRSP must support the On-demand Ranging Data and may support the Real-time Ranging Data. The RREQ shall enable one of these Ranging Data notifications or indications according to the support indicated by the RAS Features characteristic and the latency needs of the RREQ. This enables the RREQ to receive CS Procedure Data from the RRSP that supports either indications or notifications.

4.4.1 Real-time Ranging Data characteristic

The RREQ may enable Real-time Ranging Data notifications or indications if Real-time Ranging Data is supported by the RRSP, as indicated by the RAS Features characteristic, and if the RREQ is configured to receive ranging information in real time. Notifications and indications are enabled by the RREQ by writing the indication or notification bits to the Real-time Ranging Data Client Characteristic Configuration Descriptors (CCCD) (see Volume 3, Part G, Section 3.3.3.3 in [1]). After Ranging Data is available, the RRSP will start sending Real-time Ranging Data notifications or indications to the connected RREQ device that enabled notifications or indications for the characteristic, as described in Figure 4.1 and in Section 2.7.1 in [2]. The data format and segmentation procedures are specified in Section 3.2 in [2].

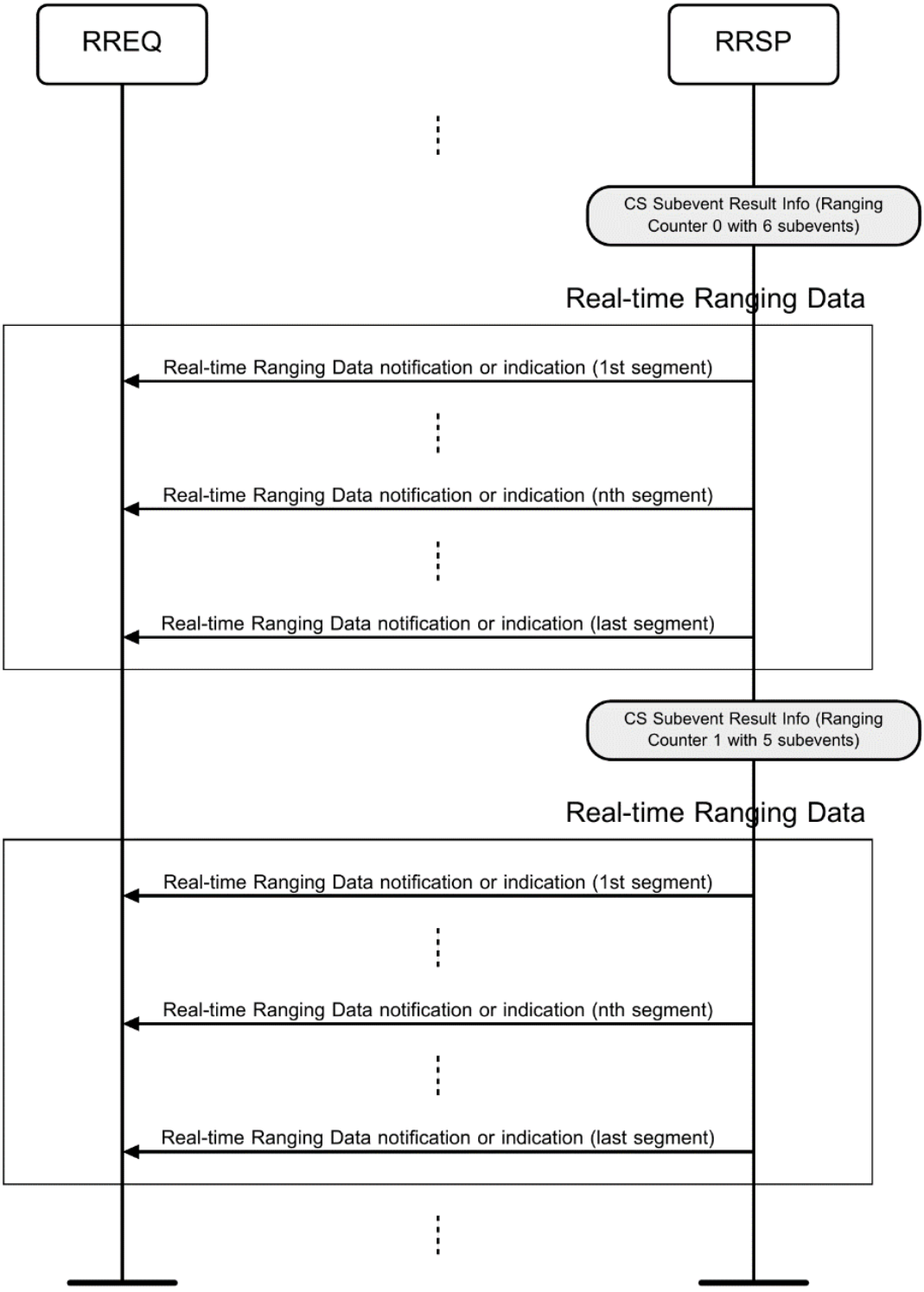

Figure 4.1: ***Message sequence chart for Real-time Ranging Data***

4.4.1.1 Real-time Ranging Data notification or indication timeouts

If the RREQ enables Real-time Ranging Data indications or notifications and does not receive a Real-time Ranging Data indication or notification within 5 seconds (or a shorter configurable timeout value) after starting the CS Procedure, then the RREQ shall disable receiving indications or notifications from the RRSP by writing a notifications or indications disabled value (see Volume 3, Part G, Section 3.3.3.3 in

[1]) to the Real-time Ranging Data CCCD, and the RREQ should notify a timeout error to the distance-measurement application.

If the RREQ does not receive a subsequent (or the last) Real-time Ranging Data indication or notification within 1 second of the previously received notification or indication, then the RREQ shall disable receiving indications or notifications from the RRSP by writing a notifications or indications disabled value (see Volume 3, Part G, Section 3.3.3.3 in [1]) to the Real-time Ranging Data CCCD, and the RREQ should notify a timeout error to the distance-measurement application.

4.4.2 On-demand Ranging Data characteristic

If the RREQ does not enable Real-time Ranging Data notifications or indications, then it shall enable On-demand Ranging Data notifications or indications.

Figure 4.2 describes the On-demand Ranging Data procedure, and the flow is specified in Section 4.4.3.

The data format and segmentation procedures are specified in Section 3.2 in [2].

After all Ranging Data is sent, the RRSP indicates a Complete Ranging Data Response message. If all the segments of an On-demand Ranging Data notification or indication were received, then the RREQ shall respond with an ACK_Ranging_Data command written to the RAS Control Point.

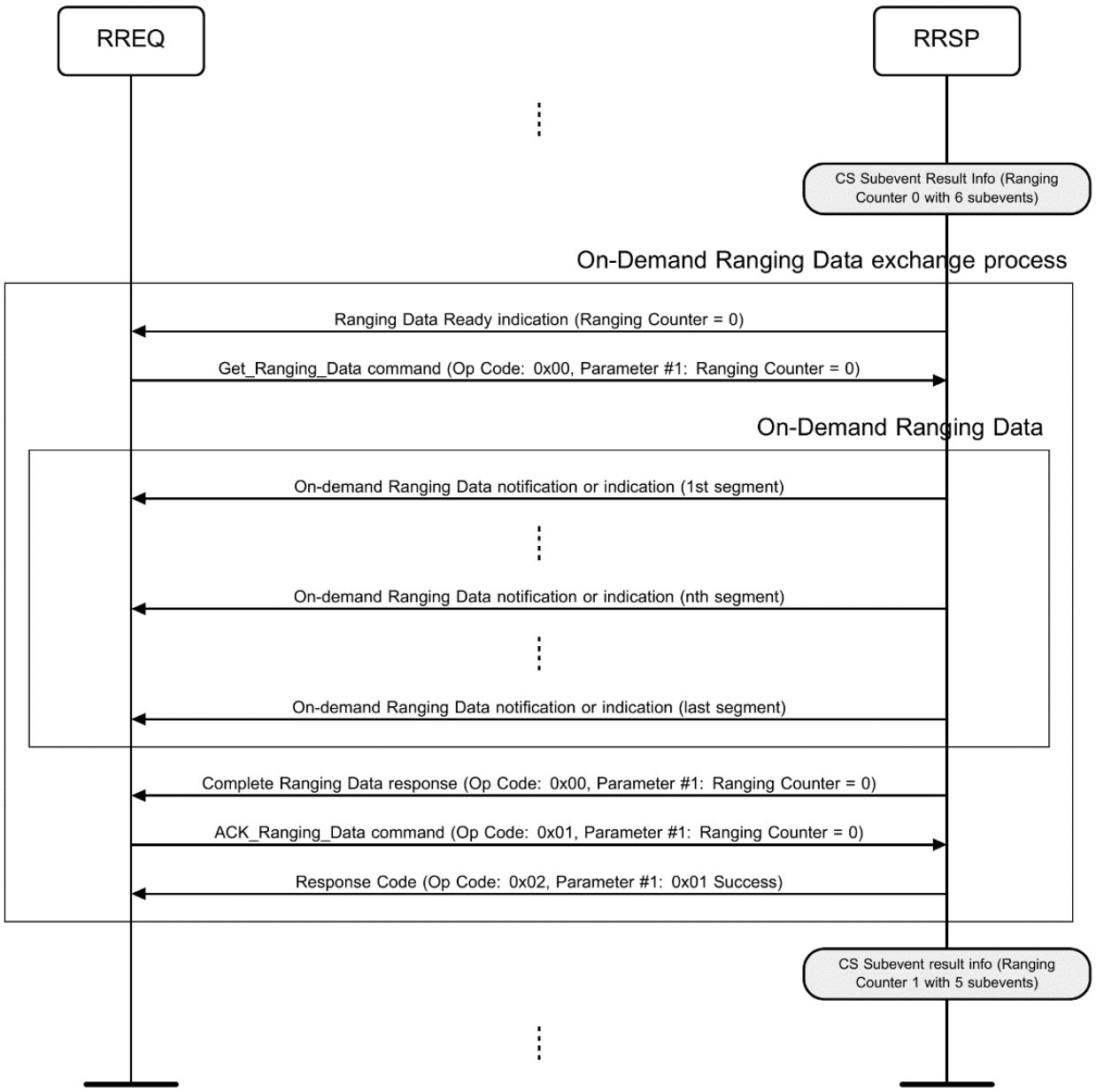

Figure 4.2: Message sequence chart for On-demand Ranging Data using RAS Control Point

4.4.2.1 Retransmission of lost Ranging Data segments

If one or more segments of an On-demand Ranging Data notification or indication were not received, then the RREQ may write a Retrieve_Lost_Procedure_Segments command to the RAS Control Point, if supported by the RRSP, and specify the missing segment(s) it needs after the Complete Ranging Data Response notification or indication was received.

If the RRSP has the requested segment in memory, then the RRSP will respond with the requested segment of the Ranging Data followed by a Complete Lost Procedure Segment Response. If the RREQ received all segments, then the RREQ shall respond with an ACK_Ranging_Data command written to the RAS Control Point. Otherwise, the RREQ may repeat this procedure until all segments were received or until the RRSP responds with an error. If the RRSP cannot locate the requested segment(s), then the RRSP will indicate the RAS Control Point with a Response Code Op Code and Response Code Value in

the Parameter set to No Records Found, and the RREQ should forward the error to the distance-measurement application to indicate an incomplete ranging result.

Figure 4.3 describes an example of the retrieval of a lost segment.

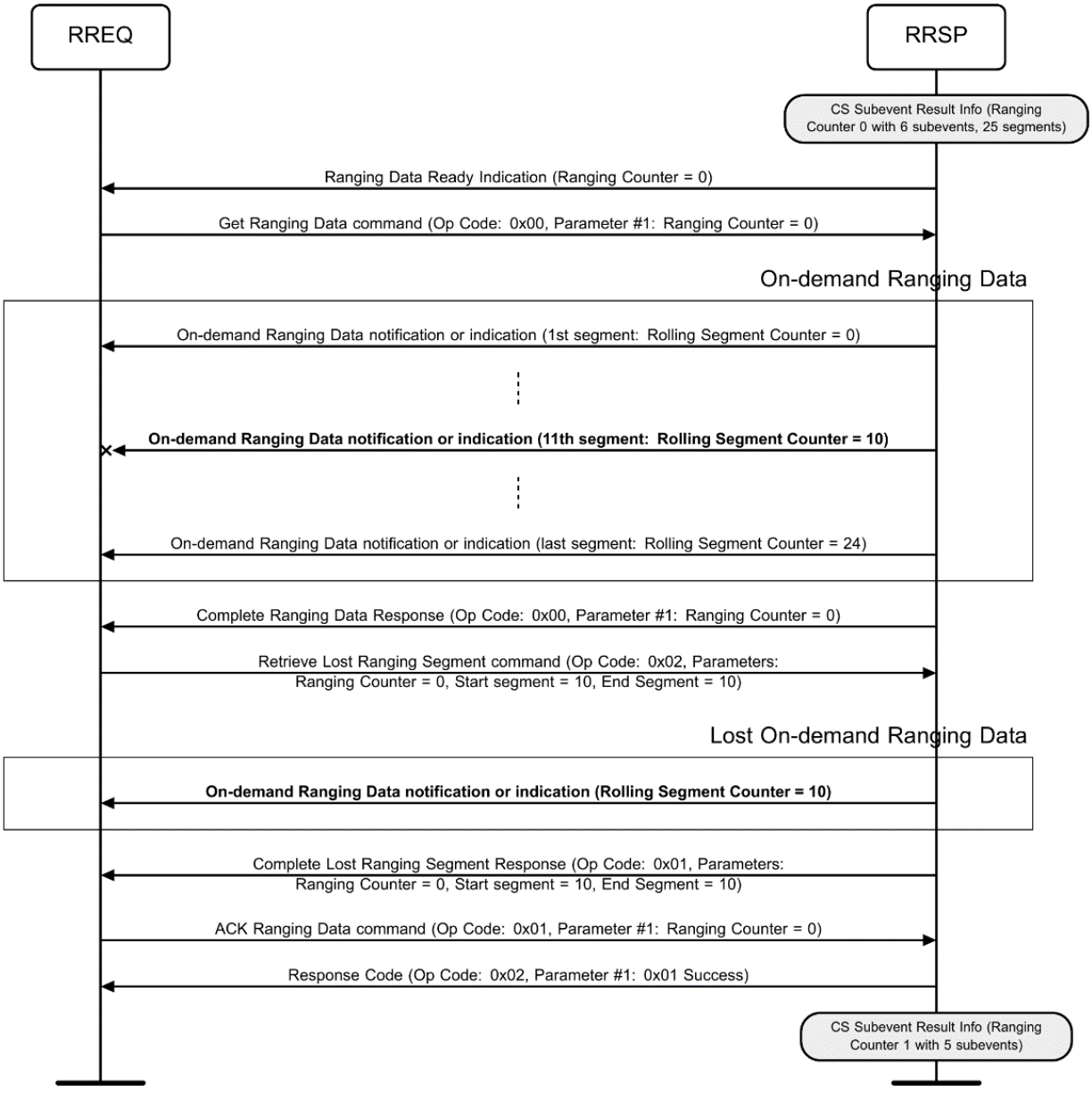

Figure 4.3: Message sequence chart for a Retrieve_Lost_Procedure_Segment command using RAS Control Point

4.4.3 Ranging Data Ready characteristic

If the RREQ enables On-demand Ranging Data notifications or indications, then the RREQ shall enable Ranging Data Ready indications, or notifications, if supported by the RRSP.

Once Ranging Data is available, the RRSP sends a Ranging Data Ready notification or indication that includes the Ranging Counter, as described in Figure 4.2 and in Section 2.7.2 in [2]. In response, the RREQ should write the Get_Ranging_Data command to the RAS Control Point, as specified in Section 3.3.2.1 in [2]. If the RREQ does not write the Get_Ranging_Data command to the RAS Control Point,

then the Ranging Data associated with the Ranging Data Ready notification might be overwritten (see Section 4.4.4).

4.4.3.1 Ranging Data Ready timeout

If the RREQ enables indications for the Ranging Data Ready characteristic and the RREQ does not receive a Ranging Data Ready indication within 5 seconds (or a shorter implementation configurable timeout value) after the distance-measurement application started the CS Procedure, then the RREQ should notify a timeout error to the distance-measurement application.

If the RRSP supports notifications for the Ranging Data Ready characteristic and notifications were enabled by the RREQ, and if the RREQ does not receive a Ranging Data Ready notification within 5 seconds (or a shorter implementation configurable timeout value) after the distance-measurement application started the CS Procedure, then the RREQ may read the Ranging Data Ready characteristic value, if supported by the RRSP, and attempt to continue the procedure. The RREQ should notify a timeout error to the distance-measurement application if attempts to continue the procedure are not successful.

4.4.4 Ranging Data Overwritten characteristic

If the RREQ enables On-demand Ranging Data notifications or indications, then the RREQ shall enable Ranging Data Overwritten indications, or notifications, if supported by the RRSP.

The RREQ will receive Ranging Data Overwritten events when some Ranging Data was lost because of being overwritten by the RRSP. This could happen when the RRSP runs out of memory (i.e., if the RREQ did not ask for the data quickly enough after it received the Ranging Data Ready notification) or when the distance-measurement application has scheduled a tight period for the CS Procedure and may need to increase the CS Procedure interval (see Volume 6, Part B, Section 4.5.18.1 in [1]).

If the RRSP supports notifications for the Ranging Data Overwritten characteristic and notifications were enabled by the RREQ, then there is a possibility that Ranging Data Overwritten notifications might get lost. The RREQ may read the Ranging Data Overwritten characteristic value, if supported by the RRSP, and attempt to recover the procedure.

The RREQ should notify a Ranging Data Overwritten error to the distance-measurement application to allow the distance-measurement application to update its configuration.

Figure 4.4 describes a possible message sequence chart when Ranging Data is overwritten by the RRSP.

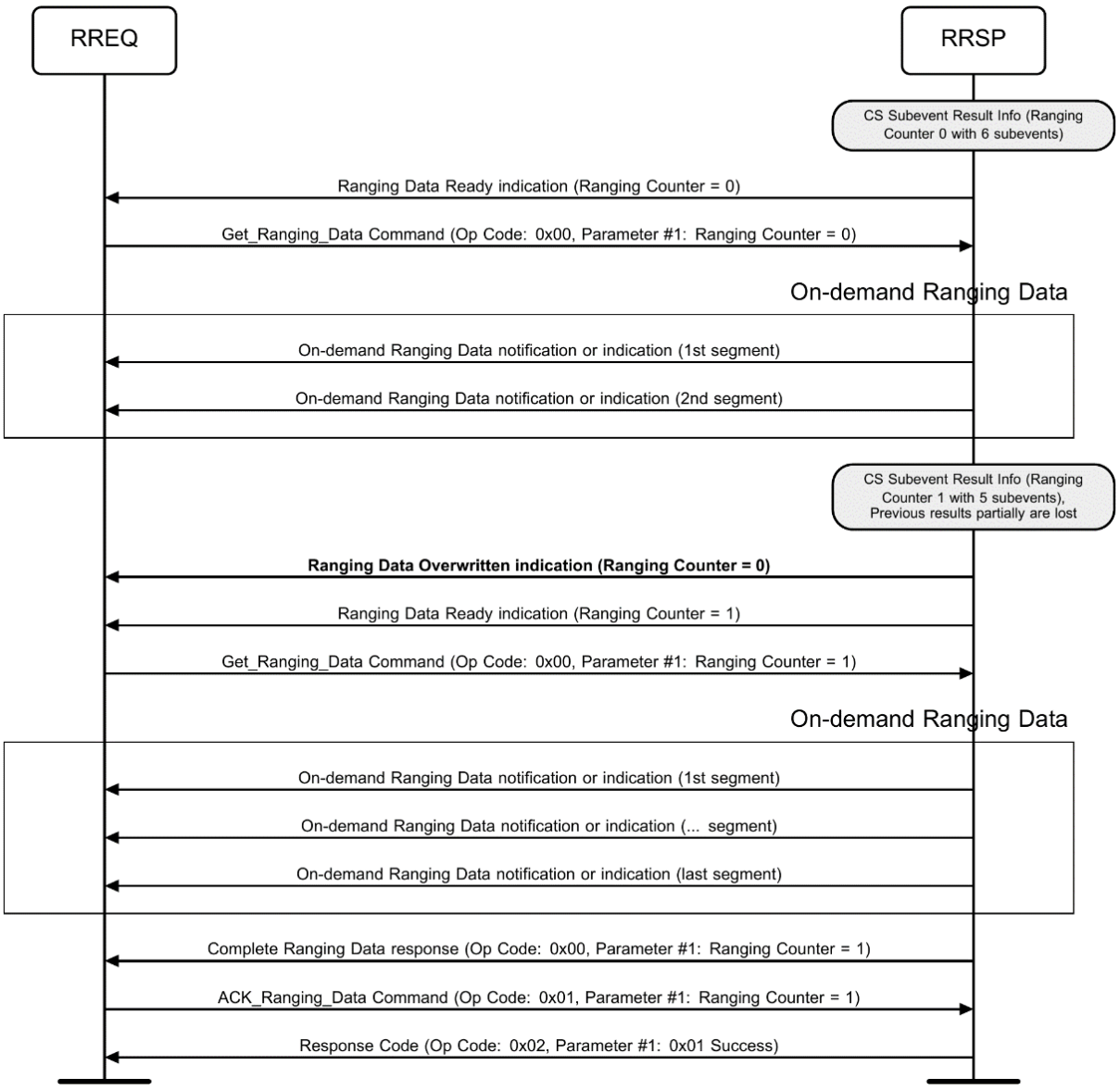

Figure 4.4: Message sequence chart for a Ranging_Data_Overwritten indication

4.4.5 Ranging Data segments received out of order

When the RRSP and RREQ establish a connection with multiple EATT bearers, Ranging Data segments might be received out of order. The RREQ should reorder the Ranging Data segments based on the Segment Index attached to each Segmentation Header (see Table 3.5 in [2]) before sending the Ranging Data to the distance-measurement application.

4.5 RAS Control Point characteristic

4.5.1 RAS Control Point characteristic write operations

The commands that the RREQ can write to the RRSP and their format are specified in Section 3.3.1 in [2].

4.5.1.1 Configuration of the Ranging Data Filter

The RREQ may configure a Ranging Data Filter to request that the RRSP filter out some of the data from the Ranging Data notifications or indications if the RRSP supports the Set_Filter command. If data filtering is needed by the RREQ and supported by the RRSP, then the RREQ shall write the Filter command to the RAS Control Point before enabling Ranging Data notifications or indications (see Section 3.3.2.4 in [2]). The RREQ shall not write the Set_Filter command after enabling Ranging Data notifications or indications. If a new filter setting is needed by the RREQ, then the RREQ shall first disable Ranging Data notifications or indications.

4.5.1.2 Abort Operation

The RREQ may request that the RRSP abort the ongoing operation (if the RRSP supports this command) by writing the Abort_Operation command to the RAS Control Point. See Section 3.3.2.5 in [2].

4.5.2 RAS Control Point characteristic indications

The RREQ shall receive and handle indications from the RRSP, which are indicated via the RAS Control Point indications as specified in Table 3.13 in [2].

4.5.2.1 RAS Control Point Complete Ranging Data Response

When the RREQ receives a RAS Control Point indication with a Response Code Op Code and Response Code Value in the Parameter set to Complete Ranging Data Response, the RREQ shall verify that all Ranging Data segments were received and shall forward the Ranging Data to the distance-measurement application for processing.

When the RRSP and RREQ establish a connection with multiple EATT bearers, the RAS Control Point indication might arrive before the last segment of the Ranging Data. If the RREQ enabled On-demand Ranging Data indications, then the RREQ should wait for the remaining Ranging Data segments to arrive. Otherwise, or if the RREQ enabled On-demand Ranging Data notifications, then the RREQ may wait for the remaining Ranging Data segments to arrive or assume some segments are missing.

If one or more segments are missing, then the RREQ may request the lost segments as specified in Section 4.4.2.1, if supported by the RAS Server.

4.5.2.2 RAS Control Point Complete Lost Ranging Data Segment Response

When the RREQ receives a RAS Control Point indication with a Response Code Op Code and Response Code Value in the Parameter set to Complete Lost Ranging Data Segment Response, it shall verify that all remote Ranging Data segments were received and shall forward the Ranging Data to the distance-measurement application for processing. If one or more segments are still missing, then the RREQ may request the lost segments as specified in Section 4.4.2.1 unless the Ranging Data Overwritten indication is sent by the RRSP (see Section 3.5 in [2]) or the RRSP responded with a RAS Control Point indication with a Response Code Op Code and Response Code Value in the Parameter set to No Records Found.

When the RRSP and RREQ establish a connection with multiple EATT bearers, the RAS Control Point indication might arrive before the last requested lost Ranging Data segment. If the RREQ enabled On-demand Ranging Data indications, then the RREQ should wait for the remaining Ranging Data segments to arrive. Otherwise, or if the RREQ enabled On-demand Ranging Data notifications, then the RREQ may either wait for the remaining Ranging Data segments to arrive or assume some segments are still missing and then request additional lost segments as specified in Section 4.4.2.1.

If the RREQ did not write a Retrieve_Lost_Ranging_Data_Segments command to the RAS Control Point, then the RREQ shall ignore this response.

4.5.3 RAS Control Point Response

The RREQ shall receive a RAS Control Point Response from the RRSP after each RAS Control Point write command. Table 3.12 in [2] specifies the Response Code Values.

Upon receiving a Success Response, the RREQ may notify the distance-measurement application about the successful operation and shall proceed to the next operation.

4.5.4 RAS Control Point procedure error and timeout handling

4.5.4.1 On-demand Ranging Data notification or indication timeouts

If the RREQ does not receive an On-demand Ranging Data indication or notification within 5 seconds after writing a Get_Ranging_Data command to the RAS Control Point, then the RREQ shall consider the request aborted and shall write an Abort command to the RAS Control Point, if supported by the RRSP. In addition, the RREQ shall notify a timeout error to the distance-measurement application.

If the RREQ does not receive a subsequent (or the last) On-demand Ranging Data indication or notification within 1 second of the previously received notification or indication, then the RREQ shall write an Abort command to the RAS Control Point, if supported by the RRSP, and notify a timeout error to the distance-measurement application.

4.5.4.2 RAS Control Point indications error handling

Error codes from the RRSP are indicated via the RAS Control Point indications with Response Code 0x02, as specified in Table 3.12 in [2].

Response Value Op Codes 0x06: Abort Unsuccessful and 0x07: Procedure Not Completed shall be forwarded to the local distance-measurement application on the RREQ.

Other error codes specified in [2] should be logged and may be related to an incorrect implementation of either the RREQ or the RRSP. These responses shall be forwarded to the local distance-measurement application on the RREQ as a fatal error that requires closing the link.

If the RREQ receives a response with an RFU Response Code Value, then it shall ignore the response. It may also notify the distance-measurement application and may log the invalid value.

4.6 Summary of GATT sub-procedures for RREQ

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

Table 4.2 summarizes GATT sub-procedure requirements.

GATT Sub-Procedure	Requirements
Discover All Primary Services	C.1
Discover Primary Services by Service UUID	C.1
Discover All Characteristic Descriptors	M
Find Included Services	M

GATT Sub-Procedure	Requirements
Discover All Characteristics of a Service	C.2
Discover Characteristics by UUID	C.2
Read Characteristic Value	M
Write Without Response	M
Notifications	M
Indications	M
Read Characteristic Descriptors	M
Write Characteristic Descriptors	M

Table 4.2: GATT sub-procedure requirements

C.1: Mandatory to support at least one of these service discovery sub-procedures; otherwise, Optional.

C.2: Mandatory to support at least one of these characteristic discovery sub-procedures; otherwise, Optional.

5 Connection establishment procedures

There are no additional requirements specified concerning connection procedures and modes for the RRSP and RREQ roles beyond those found in GAP (see Volume 3, Part C in [1]).

6 Security requirements

This section describes the security requirements for the RRSP and RREQ roles beyond those already required by RAS [2].

6.1 Bluetooth device address requirements

The RRSP and RREQ shall use a random device address as described in Volume 6, Part B, Section 1.3.2 in [1]. The RRSP and RREQ may use a Non-resolvable private address, a Resolvable Private Address (RPA), or a static device address based on its configuration, use case, and form factor. If the RRSP or the RREQ are attached to a non-stationary device, then the RRSP or RREQ should not use an address that remains constant for long periods.

6.2 General security requirements

The RRSP and RREQ shall use LE Secure Connections pairing (see Volume 3, Part H, Section 2 in [1]).

All traffic between the RRSP and RREQ, including Ranging Data exchange, commands, responses, indications, and notifications, shall be encrypted using an encryption key with a minimum of 128-bit equivalent strength.

If Passkey Entry is used for Authentication stage 1 (see Volume 3, Part H, Section 2.3.5.6.3 in [1]), then static passkeys shall not be used.

RRSP and RREQ LE Bluetooth devices that implement the GAP Peripheral role should enter Limited Discoverable mode when accepting pairing (see Volume 3, Part C, Section 9.2.3 in [1]). Alternatively, the devices should minimize the time spent operating in General Discoverable mode (see Volume 3, Part C, Section 9.2.4 in [1]) such that they are discoverable and connectable for a limited duration only following a user interaction to initiate pairing.

6.3 Out-of-band pairing

The Random Value that is generated as part of the out-of-band (OOB) authentication data (see Volume 3, Part H, Section 2.3.5.6.4 in [1]) shall meet the requirements for random generation defined in Volume 2, Part H, Section 2 in [1]. Random values and Confirm values shall be non-zero values and shall be used only once. Ephemeral Public Keys that are used for generating the Confirm values shall be used only once. If pairing fails for any reason, new OOB authentication data shall be generated. OOB authentication data may be managed and provisioned by an external application to two LE Bluetooth devices that participate in a ranging session.

The OOB authentication data format shall be constructed according to the requirements in Volume 3, Part H, Section 2.3.3 in [1]. Table 6.1 summarizes the mandatory AD types required for RAP OOB pairing (see [3] for additional details about each field). Additional data types from [3] may be included. An implementation may ignore AD types not specified in Table 6.1 without any impact to the RAP functionality. LE Bluetooth devices that use OOB pairing via Near Field Communication (NFC) shall support the OOB Authentication Data format specified in [4].

AD Type	Assigned Number	Length (in Octets)	Description
LE Bluetooth Device Address	0x1B	7	The LE Bluetooth Device Address AD type defines the device address of the local device and the address type on the LE transport. If the LE Bluetooth Device Address is not provided, then all the octets shall be set to 0. The format is defined in Section 1.16 in the Bluetooth Core Specification Supplement [5].
LE Role	0x1C	1	The LE Role AD type defines the LE role capabilities of the device. The format is defined in Section 1.17 in [5].
LE Secure Connections Confirm Value	0x22	16	The LE Secure Connections Confirm Value is a 128-bit value resulting from the f4 function specified in the Security Manager Cryptographic Toolbox (see Volume 3, Part H, Section 2.2.6 in [1]). The format is defined in Volume 3, Part H, Section 2.3.5.6.4 in [1].
LE Secure Connections Random Value	0x23	16	The LE Secure Connections Random Value is a 128-bit random value that meets the requirements for random generation defined in Volume 2, Part H, Section 2 in [1]. The format is defined in Volume 3, Part H, Section 2.3.5.6.4 in [1].

Table 6.1: RAP mandatory AD types for OOB pairing

6.4 Security requirements for BR/EDR

Basic Rate/Enhanced Data Rate (BR/EDR) transport is not supported by RAP.

7 Additional requirements for BR/EDR

BR/EDR transport is not supported by RAP.

8 Acronyms and abbreviations

Acronym/Abbreviation	Meaning
ACL	Asynchronous Connection-oriented logical transport
AD	Advertising Data
ATT	Attribute Protocol
BR/EDR	Basic Rate/Enhanced Data Rate
CCCD	Client Characteristic Configuration Descriptors
CS	Channel Sounding
EATT	Enhanced Attribute Profile
GAP	Generic Access Profile
GATT	Generic Attribute Profile
L2CAP	Logical Link Control and Adaptation Protocol
LE	Low Energy
LL	Link Layer
NFC	Near Field Communication
MTU	Maximum Transmission Unit
OOB	out-of-band
PDU	Protocol Data Unit
RAP	Ranging Profile
RAS	Ranging Service
RFU	Reserved for Future Use
RPA	Resolvable Private Address
RREQ	Ranging Requester
RRSP	Ranging Responder
UUID	Universally Unique Identifier

Table 8.1: Acronyms and abbreviations

9 References

[1] Bluetooth Core Specification, Version 6.0 or later

[2] Ranging Service, Version 1.0

[3] Bluetooth Assigned Numbers, https://www.bluetooth.com/specifications/assigned-numbers/

[4] NFC Forum, “Bluetooth® Secure Simple Pairing Using NFC, Version 1.3”, December 2020, https://nfc-forum.org/build/specifications/bluetooth-secure-simple-pairing-using-nfc/

[5] Bluetooth Core Specification Supplement, Version 12 or later