Quintic OTA Profile Guide

Confidential

Version 0.1

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

Table of Contents

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

1. Introduction

The OTA is used to upgrade the firmware of QN902x over the air.

1.1 Profile Dependencies

This profile requires the Generic Attribute Profile (GATT).

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.

1.3 Bluetooth Specification Release Compatibility

This specification is compatible with any *Bluetooth* Core Specification that includes the Generic Attribute Profile (GATT) specification and the Bluetooth Low Energy Controller specification.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

2. Configuration

2.1. Roles

The profile defines two roles: OTA Server and OTA Client.

- The OTA Server shall be a GATT server.
- The OTA Client shall be a GATT client.

2.2. Role/Service Relationships

The diagram 2.1 shows the relationships between services and the two profile roles.

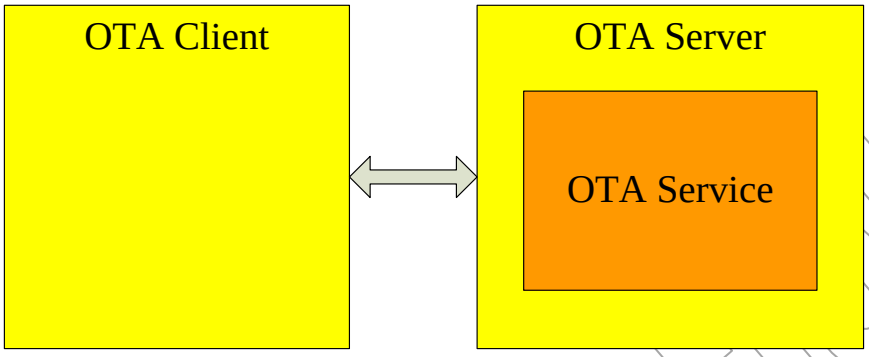


Diagram 2.1 Role / Service Relationships.

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

An OTA Server shall instantiates one and only one OTA Service.

2.3. Concurrency Limitations and Restrictions

There are no concurrency limitations or restrictions for the OTA Client and Server roles imposed by this profile.
For cases where bonding is supported multiple bonds may be supported, but is outside the scope of this profile.

2.4. Topology Limitations and Restrictions

The OTA Server shall use the GAP Peripheral role.
The OTA Client shall use the GAP Central role.

2.5. Transport Dependencies

This profile shall operate over an LE transport.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

3. OTA Server Role Requirements

The OTA Server shall instantiate one and only one OTA Service.

Table 3.1 OTA Server Service Requirements

Service	Requirement
OTA Service	Mandatory

3.1 Incremental OTA Service Requirements

This section describes additional Server requirements beyond those defined in the OTA Server Service.

3.1.1. Service UUIDs AD Type

While in a GAP Discoverable Mode for initial connection to a Client, the OTA Server should include the OTA Service UUID defined in *Table 3.1* in the Service UUIDs AD type field of the advertising data. This enhances the user experience as a server may be identified by the client before initiating a connection.

3.1.2. Local Name AD Type

For enhanced user experience an OTA Server may include the Local Name in its Advertising Data or Scan Response data.

3.2 Service Characteristics

The following characteristics are exposed in the OTA Service. Unless otherwise specified, only one instance of each characteristic is permitted within this service.

Table 3.2 OTA Service characteristics

Characteristic Name	Requirement	Mandatory Properties	Optional Properties	Security Permissions	UUID
OTA Service Declaration (Primary Service)	M	Read		None.	0xFEE8
TX Char. Declaration	M	Read		None.	
TX Char. Value	M	Notify		None.	UUID*
TX Client Char. Configuration Descriptor	M	Read		None.	
TX User Descriptor	M	Read		None.	
RX Char. Declaration	M	Read		None.	
RX Char. Value	M	Write Without Response		None.	UUID**

**: The UUID of TX characteristic is 0x003784CFF7E355B46C4C9FD140100A16*

***: The UUID of RX characteristic is 0x013784CFF7E355B46C4C9FD140100A16*

Notes: Security Permissions of "None" means that this service does not impose any requirements.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

4. OTA Client Role Requirements

The Client shall support the OTA Service.

Table 4.1 OTA Client Service Requirements

Service	Requirement
OTA Service	Mandatory

This section describes the profile procedure requirements for an OTA Client.

Table 4.2 OTA Client Requirements

Profile Requirement	Section	Support
Service Discovery	4.2	Mandatory
- OTA Server Service Discovery	4.2.1	Mandatory
Characteristic Discovery	4.3	Mandatory
- OTA Server Service Characteristic Discovery	4.3.1	Mandatory
Transmit Command to Server	4.4	Mandatory
Receive Response from Server	4.5	Mandatory

4.1. GATT Sub-Procedure Requirements

Requirements in this section represent a minimum set of requirements for a Client. Other GATT sub-procedures may be used if supported by both Client and Server.
Table 4.3 summarizes additional GATT sub-procedure requirements beyond those required by all GATT Clients.

Table 4.3 Additional GATT Sub-Procedure Requirements

GATT Sub-Procedure	OTA Client Requirements
Discover All Primary Services	C1
Discover Primary Services by Service UUID	C1
Discover All Characteristics of a Service	C2
Discover Characteristics by UUID	C2
Discover All Characteristic Descriptors	M
Write Characteristic Value	M
Notifications	M

C1: Mandatory to support at least one of these sub-procedures.

C2: Mandatory to support at least one of these sub-procedures.

4.2. Service Discovery

The Client 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. Recommended fast connection parameters and procedures for connection establishment are defined in Section 6.2.2.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

4.2.1. OTA Server Service Discovery

The Client shall perform primary service discovery to discover the OTA Server Service.

4.3. Characteristic Discovery

As required by GATT, the Client must be tolerant of additional optional characteristics in the service records of services used with this profile.

4.3.1. OTA Server Service Characteristic Discovery

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

4.3.1.1. TX Characteristic

The TX is relative to the server-side.
The Client shall discover the TX characteristic.
The Client shall discover the *Client Characteristic Configuration* descriptor of the TX characteristic.

4.3.1.2. RX Characteristic

The RX is relative to the server-side.
The Client shall discover the RX characteristic.

4.4. Transmit Command to Server

The RX characteristic is used to transmit command from client to server. Its maximum length is 20 bytes. The RX characteristic is treated as sequence which is bunched into a large buffer. The buffer is defined in *Diagram 4.1*:

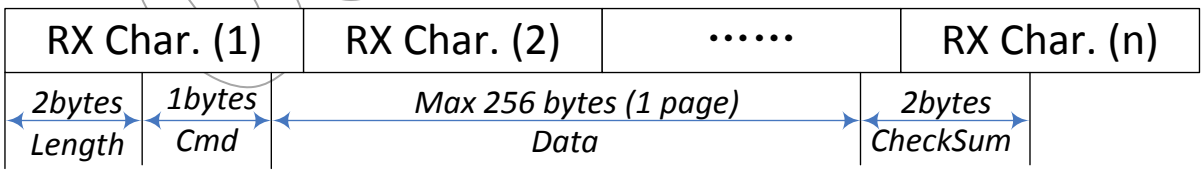


Diagram 4.1 RX characteristic sequence design

4.4.1. Parameter Length and Checksum

The range of checksum and length is from “Command” to “Data”.
The checksum is simply the sum value.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

4.4.2. Parameter Command and Data

There are four commands in the OTA profile. The *table 4.4* shows those commands.

Table 4.4 Transmit command

Command	Name	Description	Response
0x01	OTA_CMD_IND_FW_INFO	Indicate firmware information command	4.5.2.1
0x02	OTA_CMD_IND_FW_DATA	Indicate firmware data command	4.5.2.2
0x03	OTA_CMD_REQ_VERIFY_FW	Request to verify firmware data command	4.5.2.3
0x04	OTA_CMD_REQ_EXEC_FW	Request to execute new firmware command	None.

4.4.2.1. OTA_CMD_IND_FW_INFO

The data of this command is shown in *table 4.5*.

Table 4.5 The data of indicate firmware information command

version	Firmware size	Firmware CRC16	Reserved
2bytes	2bytes	2bytes	10bytes

The firmware CRC16 is calculated by the total original firmware. The CRC16 table is shown in *Appendix A*.
The Reserved section should be set to 0x00.
When enable the encryption, this packet should be encrypted by AES128.
The command can be transmitted at any time. If the OTA Server reset or disconnect, only this command can be transmitted.
The response of this command is shown in section *4.5.2.1*

4.4.2.2. OTA_CMD_IND_FW_DATA

The data of this command is shown in *table 4.6*.

Table 4.6 The data of indicate firmware data command

Firmware data
Max 256 bytes

The firmware data length should be 256 bytes except the last part of the firmware. This length can make the transmission to reach maximum efficiency.
When enable the encryption, this section should be encrypted by AES128. So the length of firmware data is must be integer multiple of 16.
The command can only be transmitted when the OTA_CMD_IND_FW_INFO command is responded by OTA_RSP_SUCCESS. Otherwise, it will be ignored by OTA Server.
The response of this command is shown in section *4.5.2.2*

4.4.2.3. OTA_CMD_REQ_VERIFY_FW

There is no data section in this command.
The command can only be transmitted when all firmware data is sent, in other word, the response section “Received firmware data length” value of OTA_CMD_IND_FW_INFO or

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

OTA_CMD_IND_FW_DATA command is greater than or equal to the command section "Firmware size" value of OTA_CMD_IND_FW_INFO command. Otherwise, it will be ignored by OTA Server.
The response of this command is shown in section 4.5.2.3

4.4.2.4. OTA_CMD_REQ_EXEC_FW

There is no data section in this command.
The command can only be transmitted when the OTA_CMD_REQ_VERIFY_FW command is responded by OTA_RSP_SUCCESS. Otherwise, it will be ignored by OTA Server.
There is no response in this command.

4.5. Receive Response from Server

The TX characteristic is used to Receive response from server by client.
The volume of TX characteristic value is 20 bytes.

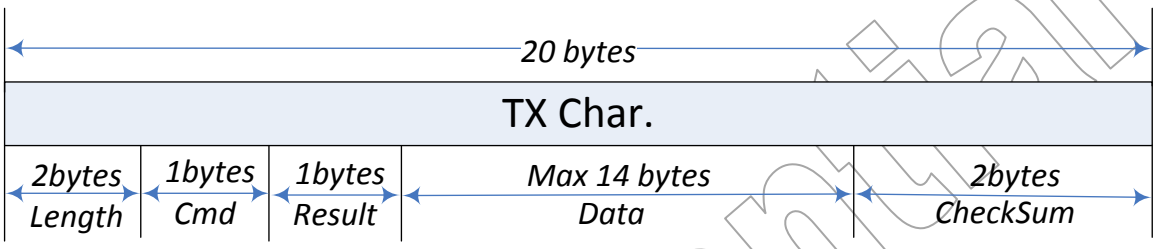


Diagram 4.2 TX characteristic designs

4.5.1. Parameter Length and Checksum

The range of checksum and length is from "Command" to "Data".
The checksum is simply the sum value.

4.5.2. Parameter Command, Result and Data

The command response is same as its command which is shown in *table 4.4.*
The result of response is listed in *table 4.7*.

Table 4.7 Result of response

Command	Name	Description
0x00	OTA_RSP_SUCCESS	Process command successfully
0x01	OTA_RSP_PKT_CHECKSUM_ERROR	Current packet checksum error
0x02	OTA_RSP_PKT_LEN_ERROR	Current packet length overflow or equal to 0
0x03	OTA_RSP_DEVICE_NOT_SUPPORT_OTA	Device don't support OTA
0x04	OTA_RSP_FW_SIZE_ERROR	OTA firmware size overflow or equal to 0
0x05	OTA_RSP_FW_VERIFY_ERROR	OTA firmware verify error

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

4.5.2.1. Response for OTA_CMD_IND_FW_INFO

The data of this response command is shown in *table 4.8*.

Table 4.8 the data of indicate firmware information response command

Received firmware data length
2 bytes

The received firmware data length is indicated that the OTA server has received how many firmware data successfully. The OTA client can use this information to resume broken transmission.

4.5.2.2. Response for OTA_CMD_IND_FW_DATA

The data of this response command is shown in *table 4.9*.

Table 4.9 the data of indicate firmware data response command

Received firmware data length
2 bytes

The response data is same as section 4.5.2.1

4.5.2.3. Response for OTA_CMD_REQ_VERIFY_FW

There is no data section in this command.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

4.6. Communication Procedure

The OTA communication procedure is shown from *figure 4.1* to *figure 4.4*.
The *figure 4.1* is shown the successful OTA procedure, and the other three figures are shown the abnormal condition. The OTA Client should handle the abnormal condition.

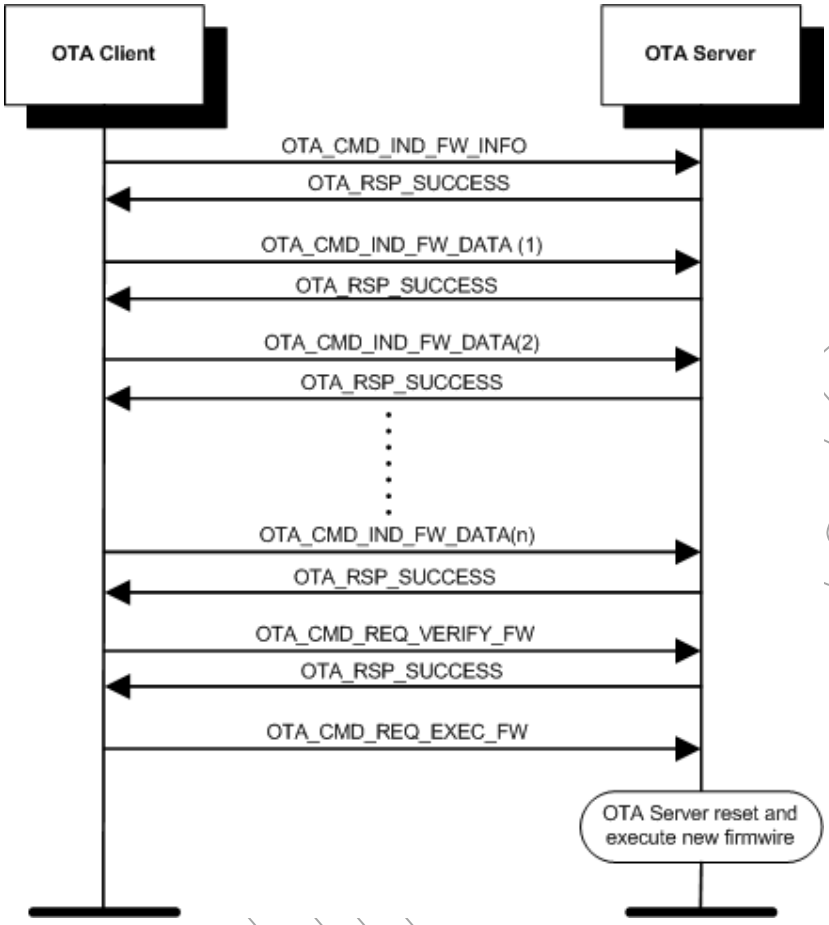


Figure 4.1 OTA procedure is successful

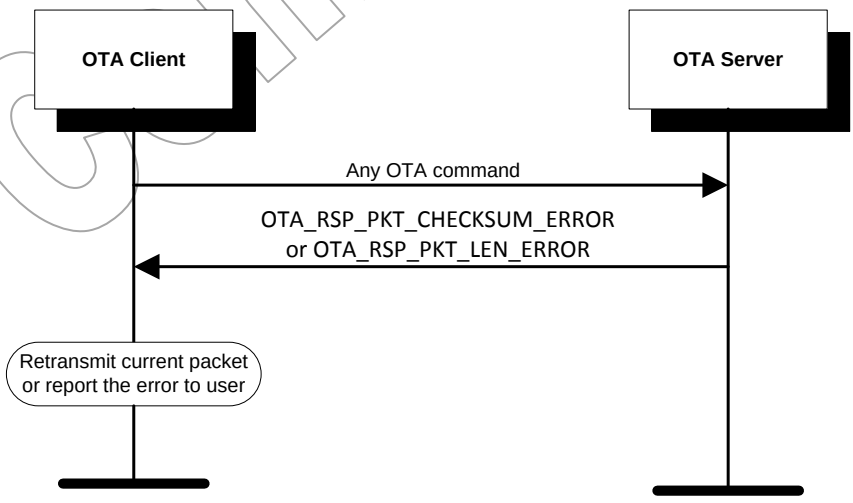


Figure 4.2 OTA procedure is fail: Packet is error

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

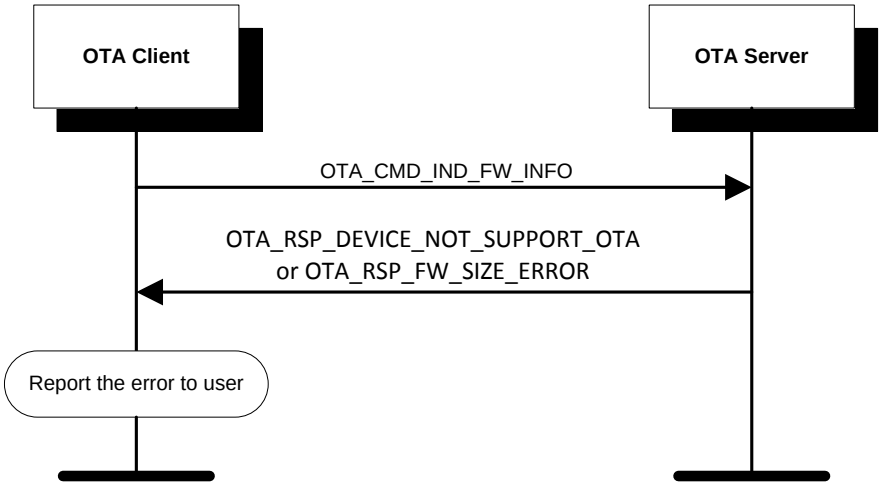
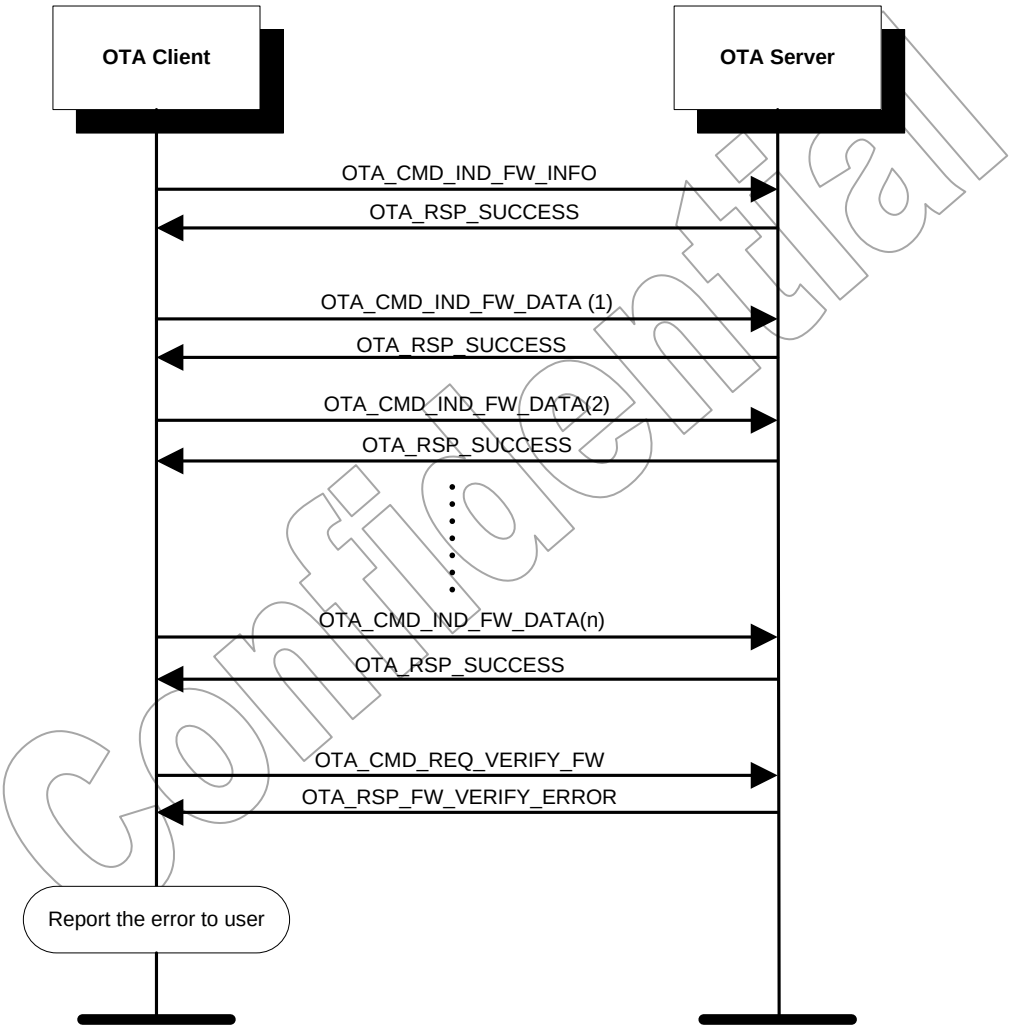


Figure 4.3 OTA procedure is fail: Device doesn't support OTA or firmware size error



Confidential

Figure 4.4 OTA procedure is fail: Firmware verify fail

4.7. Bit Ordering

The bit ordering used for all parameter shall be little-endian.

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

5. Security

In order to prevent hacker to attack and protect data security over air, the communication data should be encrypted. The encryption algorithm is AES128.
The OTA Client should use AES128 decryption algorithm to encrypt and the OTA Server should use AES128 encryption algorithm to decrypt. And this may be some mouthful. Both sides should be the same key.

5.1 Encrypt Section

If enable the encryption, the data section of OTA_CMD_IND_FW_INFO and OTA_CMD_IND_FW_DATA command should be encrypted.

5.2 Upgrade File Format

The *Diagram 5.1* is shown the upgrade file format. If enable the encryption, the file is encrypted by this format before do OTA. If the original firmware is not integer multiple of 16, it should be complemented by the addition of 0xFF. The OTA Client should parse the upgrade file and transmit them through OTA procedure.

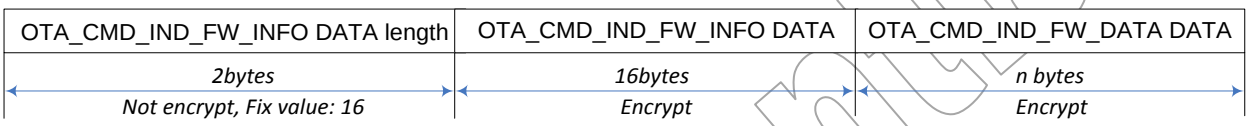


Diagram 5.1 Upgrade file format

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

6. Connection Establishment

This section describes the connection establishment used by a Client and Server in certain scenarios.

6.1 OTA Server Connection Establishment

6.1.1 Device Discovery

The Server should use the GAP *Limited Discoverable Mode* when establishing an initial connection.

6.1.2 Connection Procedure

This procedure is used for connection establishment when the Server connects to a Client to which it is not bonded. This may be initiated either through user interaction or autonomously when the Server has a notification or indication is pending.
It is recommended that the Server advertises using the parameters in *Table 5.1.*
The interval values in the first row are designed to attempt fast connection during the first 30 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.

Table 5.1 Recommended Advertising Interval Values

Advertising Duration	Parameter	Value
First 30 seconds (fast connection)	Advertising Interval	20 ms to 30 ms
After 30 seconds (reduced power)	Advertising Interval	1 s to 2.5 s

The advertising interval and time to perform advertising should be configured with consideration for user expectations of connection establishment time.
The Server shall accept any valid values for connection interval and connection latency set by the Client until service discovery and encryption is complete. Only after that should the Server change to the preferred connection parameters that best suits its use case.

6.2 OTA Client Connection Establishment

6.2.1 Device Discovery

The Client should use the GAP *Limited Discovery Procedure* to discover a Server.

6.2.2 Connection Procedure

This procedure is used for connection establishment when the Client connects to a Server to which it is not bonded. This may be initiated either through user interaction or autonomously when a Client requires from a Server.
A Client may use one of the following GAP connection procedures based on its connectivity requirements:

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

- *General Connection Establishment Procedure*. The Client may use this procedure when it requires upgrading firmware from Servers. This procedure allows a Client to connect to a Server discovered during a scan without using the white list.
- *Direct Connection Establishment Procedure*. The Client may use this procedure when it requires upgrading firmware from a single Server.
- *Auto Connection Establishment Procedure*. This procedure will automatically connect to a Server in the white list.
- *Selective Connection Establishment Procedure*. The Client may use this procedure when it requires upgrading firmware from Servers. This procedure allows a Client to connect to a Server discovered during a scan while using the white list.

The Client should use the recommended scan interval and scan window values shown in *Table 5.2*. For the first 30 seconds (or optionally continuously for mains powered devices), the Client should use the first scan window / scan interval pair to attempt fast connection. However, if a connection is not established within that time, the Client should switch to one of the other scan window / scan interval options as defined below to reduce power consumption.

Table 5.2 Recommended Scan Interval and Scan Window Values

Advertising Duration	Parameter	Value
First 30 seconds (fast connection)	Scan Interval	30ms to 60ms
	Scan Window	30ms
After 30 seconds (reduced power) - Option 1	Scan Interval	1.28s
	Scan Window	11.25ms
After 30 seconds (reduced power) - Option 2	Scan Interval	2.56s
	Scan Window	11.25ms

6.2.3 Connection Interval

To avoid very long service discovery and upgrade times, the OTA Client should use the connection intervals defined in *Table 5.3* in the connection request.

Table 5.3 Recommended Connection Interval Values

Connection Interval	Value
Minimum Connection Interval	18.75 ms
Maximum Connection Interval	30 ms

At any time a lower latency is required, for example to perform 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 5.3* and a connection latency of zero. This fast connection interval should be maintained as long as low latency is required. The Server doesn't use the GAP *Connection Parameter Update* procedure to update the connection interval.

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

7. Appendix A: CRC16 table

```
const uint16_t crc16_table[256] =
{
    0x0000L, 0x1021L, 0x2042L, 0x3063L, 0x4084L, 0x50A5L, 0x60C6L, 0x70E7L,
    0x8108L, 0x9129L, 0xA14AL, 0xB16BL, 0xC18CL, 0xD1ADL, 0xE1CEL, 0xF1EFL,
    0x1231L, 0x0210L, 0x3273L, 0x2252L, 0x52B5L, 0x4294L, 0x72F7L, 0x62D6L,
    0x9339L, 0x8318L, 0xB37BL, 0xA35AL, 0xD3BDL, 0xC39CL, 0xF3FFL, 0xE3DEL,
    0x2462L, 0x3443L, 0x0420L, 0x1401L, 0x64E6L, 0x74C7L, 0x44A4L, 0x5485L,
    0xA56AL, 0xB54BL, 0x8528L, 0x9509L, 0xE5EEL, 0xF5CFL, 0xC5ACL, 0xD58DL,
    0x3653L, 0x2672L, 0x1611L, 0x0630L, 0x76D7L, 0x66F6L, 0x5695L, 0x46B4L,
    0xB75BL, 0xA77AL, 0x9719L, 0x8738L, 0xF7DFL, 0xE7FEL, 0xD79DL, 0xC7BCL,
    0x48C4L, 0x58E5L, 0x6886L, 0x78A7L, 0x0840L, 0x1861L, 0x2802L, 0x3823L,
    0xC9CCL, 0xD9EDL, 0xE98EL, 0xF9AFL, 0x8948L, 0x9969L, 0xA90AL, 0xB92BL,
    0x5AF5L, 0x4AD4L, 0x7AB7L, 0x6A96L, 0x1A71L, 0x0A50L, 0x3A33L, 0x2A12L,
    0xDBFDL, 0xCBDCL, 0xFBBFL, 0xEB9EL, 0x9B79L, 0x8B58L, 0xBB3BL, 0xAB1AL,
    0x6CA6L, 0x7C87L, 0x4CE4L, 0x5CC5L, 0x2C22L, 0x3C03L, 0x0C60L, 0x1C41L,
    0xEDAEL, 0xFD8FL, 0xCDECL, 0xDDCDL, 0xAD2AL, 0xBD0BL, 0x8D68L, 0x9D49L,
    0x7E97L, 0x6EB6L, 0x5ED5L, 0x4EF4L, 0x3E13L, 0x2E32L, 0x1E51L, 0x0E70L,
    0xFF9FL, 0xEFBEL, 0xDFDDL, 0xCFFCL, 0xBF1BL, 0xAF3AL, 0x9F59L, 0x8F78L,
    0x9188L, 0x81A9L, 0xB1CAL, 0xA1EBL, 0xD10CL, 0xC12DL, 0xF14EL, 0xE16FL,
    0x1080L, 0x00A1L, 0x30C2L, 0x20E3L, 0x5004L, 0x4025L, 0x7046L, 0x6067L,
    0x83B9L, 0x9398L, 0xA3FBL, 0xB3DAL, 0xC33DL, 0xD31CL, 0xE37FL, 0xF35EL,
    0x02B1L, 0x1290L, 0x22F3L, 0x32D2L, 0x4235L, 0x5214L, 0x6277L, 0x7256L,
    0xB5EAL, 0xA5CBL, 0x95A8L, 0x8589L, 0xF56EL, 0xE54FL, 0xD52CL, 0xC50DL,
    0x34E2L, 0x24C3L, 0x14A0L, 0x0481L, 0x7466L, 0x6447L, 0x5424L, 0x4405L,
    0xA7DBL, 0xB7FAL, 0x8799L, 0x97B8L, 0xE75FL, 0xF77EL, 0xC71DL, 0xD73CL,
    0x26D3L, 0x36F2L, 0x0691L, 0x16B0L, 0x6657L, 0x7676L, 0x4615L, 0x5634L,
    0xD94CL, 0xC96DL, 0xF90EL, 0xE92FL, 0x99C8L, 0x89E9L, 0xB98AL, 0xA9ABL,
    0x5844L, 0x4865L, 0x7806L, 0x6827L, 0x18C0L, 0x08E1L, 0x3882L, 0x28A3L,
    0xCB7DL, 0xDB5CL, 0xEB3FL, 0xFB1EL, 0x8BF9L, 0x9BD8L, 0xABBBL, 0xBB9AL,
    0x4A75L, 0x5A54L, 0x6A37L, 0x7A16L, 0x0AF1L, 0x1AD0L, 0x2AB3L, 0x3A92L,
    0xFD2EL, 0xED0FL, 0xDD6CL, 0xCD4DL, 0xBDAAL, 0xAD8BL, 0x9DE8L, 0x8DC9L,
    0x7C26L, 0x6C07L, 0x5C64L, 0x4C45L, 0x3CA2L, 0x2C83L, 0x1CE0L, 0x0CC1L,
    0xEF1FL, 0xFF3EL, 0xCF5DL, 0xDF7CL, 0xAF9BL, 0xBFBAL, 0x8FD9L, 0x9FF8L,
    0x6E17L, 0x7E36L, 0x4E55L, 0x5E74L, 0x2E93L, 0x3EB2L, 0x0ED1L, 0x1EF0L,
};
```

Quintic Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)

Release History

REVISION	CHANGE DESCRIPTION	DATE
0.1	Initial release	2014-05-01

Confidential

Copyright ©2013-2014 by Quintic Corporation
Confidential Information contained herein is covered under Non-Disclosure Agreement (NDA)