Authentication Service

v0.5

Core Team

2024-10-30

Contents

1 Introduction

The Authentication Service (AS) is a GATT service that leverages cryptographic algorithms and protocols to secure the pairing process of the Munic dongle

Therefore, the AS Server shall evaluate each request from the AS Client that intends to interact with the dongle. The AS Server is responsible for verifying the information security controls.

1.1 Byte transmission order

All characteristics used with this service shall be transmitted with the least significant octet (LSO) first (i.e., little endian). The least significant octet is identified in the characteristic definitions on the Bluetooth SIG Assigned Numbers webpage.

1.2 Service dependencies

AS is not dependent upon any other services.

1.3 Bluetooth Core Specification release compatibility

This specification is compatible with any Bluetooth Core Specification, Version 4.2 or later that includes GATT.

1.4 Concatenation

This document uses the symbol `||` to denote concatenation of bit and byte strings. Therefore, `x || y` is the string `x` concatenated with string `y`. If `x` is `TEXT1-` and `y` is `TEXT2`, then `x || y` is `TEXT1-TEXT2`.

2 Service

The Authentication Service is instantiated as a Primary Service.

The service universally unique identifier (UUID) is set to `0000183D-0000-1000-8000-00805F9B34FB`.

3 Authentication control overview

The AS exposes the following characteristics:

Characteristic	UUID	Mandatory Properties
Payload	`8ba5d3a5-b597-4ff7-ae8d-6a47b34c6d88`	Write
Push	`8ba5d3a6-b597-4ff7-ae8d-6a47b34c6d88`	Write

To initiate the authentication process, the client first writes a token to the payload characteristic. This token contains the necessary authentication information. Subsequently, the client writes a value of 1 to the push characteristic, signaling the server to process the authentication request.

3.1 Segmentation

The Authentication Service does not place a limit on the size of the payload Data.

If the total size of the ATT header and payload exceeds the negotiated ATT MTU, the payload must be fragmented into smaller segments. Each segment, including the ATT header, should be no larger than the MTU, which has a maximum value of 517 bytes.

The following is a high-level description of the segmentation procedure.

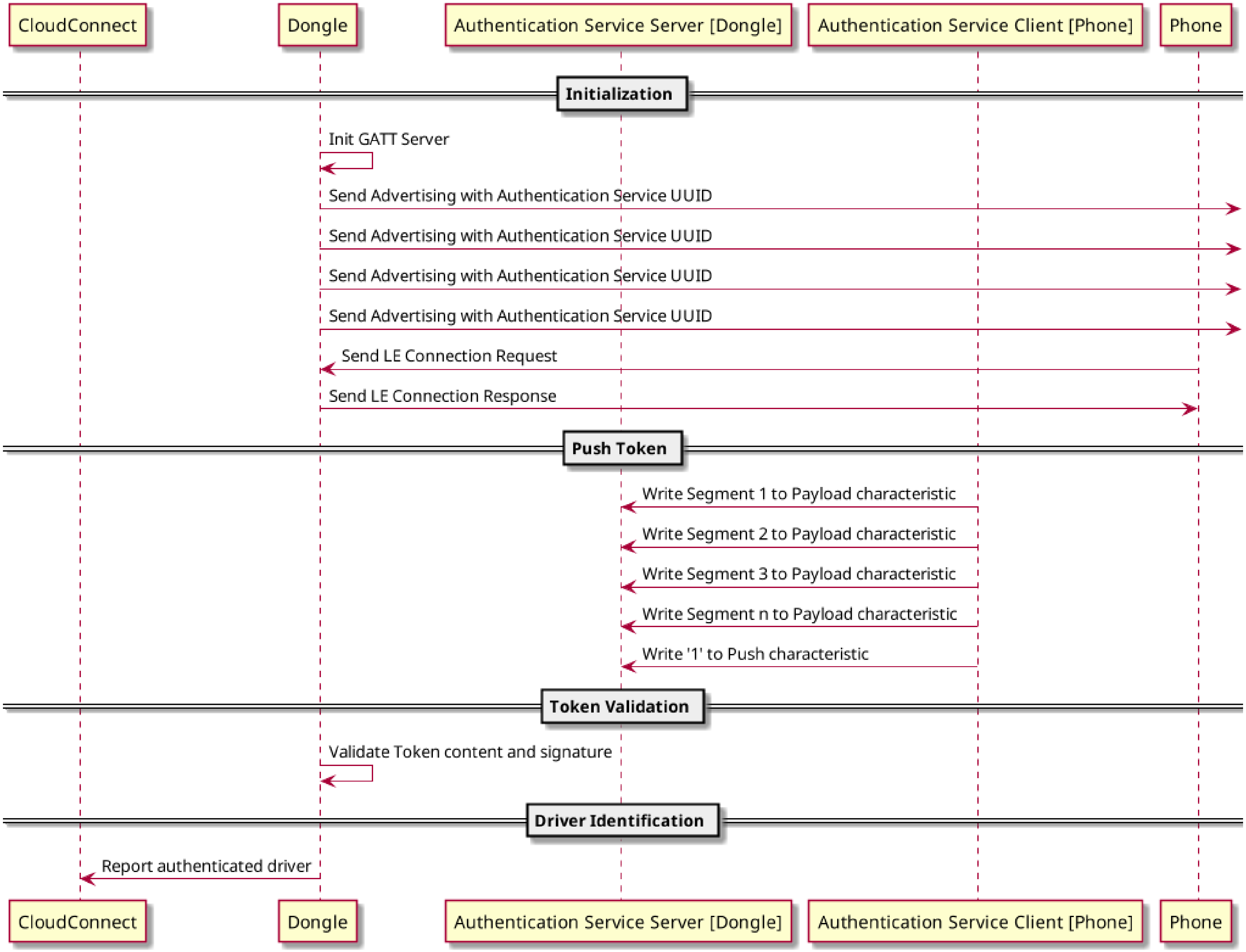
CloudConnect
Dongle
Authentication Service Server [Dongle]
Authentication Service Client [Phone]
Phone
Initialization
Init GATT Server
Send Advertising with Authentication Service UUID
Send Advertising with Authentication Service UUID
Send Advertising with Authentication Service UUID
Send Advertising with Authentication Service UUID
Send LE Connection Request
Send LE Connection Response
Push Token
Write Segment 1 to Payload characteristic
Write Segment 2 to Payload characteristic
Write Segment 3 to Payload characteristic
Write Segment n to Payload characteristic
Write '1' to Push characteristic
Token Validation
Validate Token content and signature
Driver Identification
Report authenticated driver
CloudConnect
Dongle
Authentication Service Server [Dongle]
Authentication Service Client [Phone]
Phone

Figure 1: Authentication Service

1. The Payload form the characteristic value.
2. If the size of the characteristic value and the ATT headers exceed the ATT MTU (517 bytes), the Payload field is segmented to segments with a maximum size of 512 bytes.
3. All segments of the payload are sent in sequence.
4. A `1` value is written to the Push characteristic.
5. The payload is reassembled by the AS Server, and then the characteristic value is processed.

Note: The segmentation procedure does not require the segmentation of the payload to coincide with field boundaries.

3.2 Abort procedure

If the Abort opcode `2` is written to the AS Push characteristic, then the AS Server shall stop all procedures that are in progress and drop all received chunks.