Authentication Developer Guide

v0.5

Core Team

2024-10-30

Contents

1 Introduction **3**

2 Dongle identification **3**

2.1 Advertising Content 5

2.2 Advertising Data 5

2.3 Scan Response Data 5

3 LE Connection **6**

1 Introduction

Driver identification is secured through token-based authentication. A mobile application installed on the driver's phone regularly retrieves a valid token from the authentication server.

This token is then transmitted to the dongle via a Bluetooth LE connection. The dongle validates the token to authenticate the driver's identity. The dongle periodically sends connection status reports to the backend server.

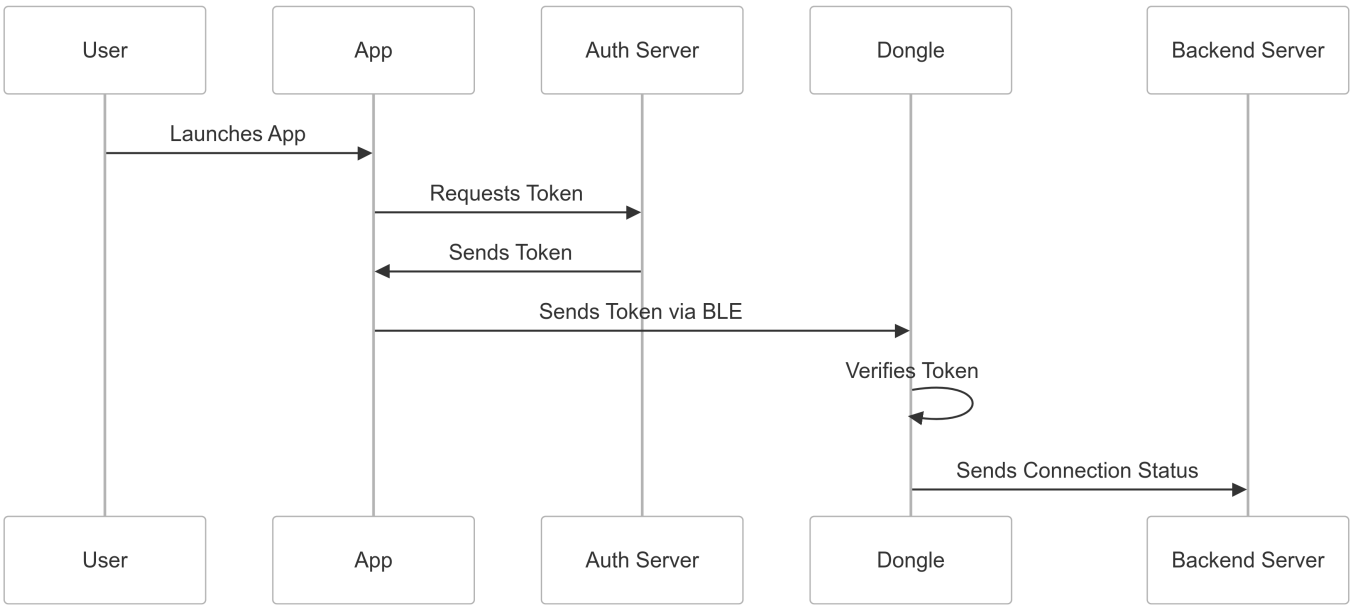

Figure 1: Authentication Overview

2 Dongle identification

The phone app initiates a Bluetooth LE scan, filtering for devices with a device name prefix of 'MUNIC_' and a specific advertising service UUID to locate the dongle.

The dongle Bluetooth name is configurable, by default is `MUNIC_<The serial number><The IMEI last 2 digits>`. See Nearby-Devices-App-Configuration for more details.

The advertising record contains a service UUID `0000183D-0000-1000-8000-00805F9B34FB` using the advertising record type `Complete List of 128-bit Service Class UUIDs` (see Bluetooth Assigned Numbers)

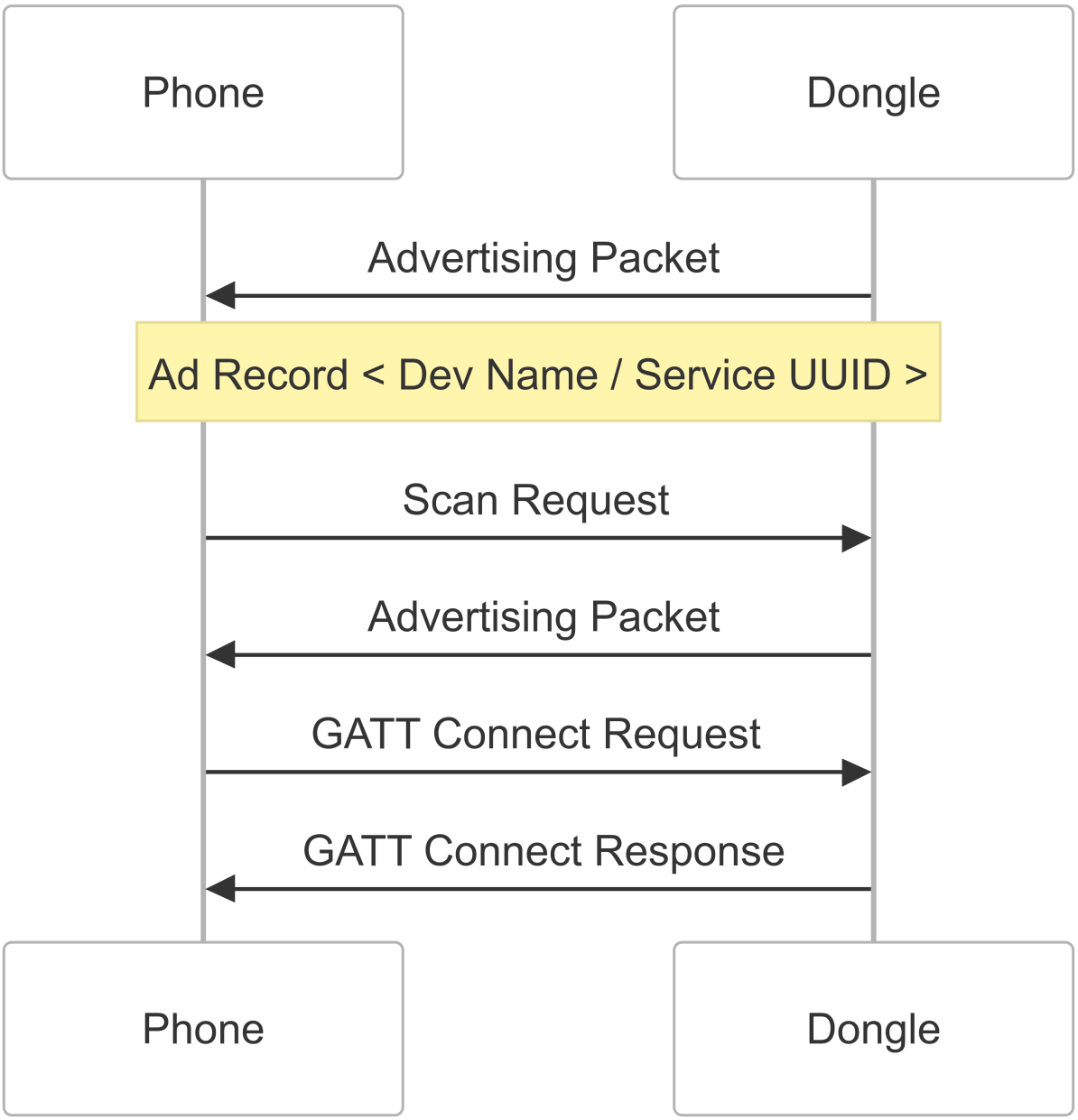

Figure 2: Dongle Identification

2.1 Advertising Content

In Bluetooth Low Energy, devices advertise their presence using two types of data: Advertising Data and Scan Response Data.

Advertising Data: This is a short, concise packet of information that a device broadcasts periodically to announce its presence.

Scan Response Data: This is a longer, more detailed packet of information that a device sends in response to a scan request.

2.2 Advertising Data

The dongle advertising Data includes:

- List of services offered `Complete List of 128-bit Service Class UUIDs`
- Connection parameters `Flags`

`Advertising data`

`11070000183D00001000800000805F9B34FB020104`

Service UUID

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

`Service UUID packet`

`11070000183D00001000800000805F9B34FB`

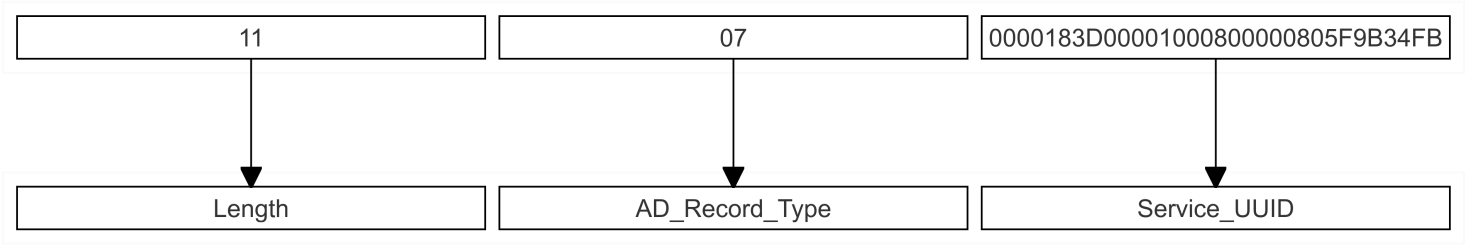

Figure 3: Advertising Data Part 1

Flags

The used flag is `BR/EDR Not Supported`, which means that the peer needs to initiate the connection over a LE link.

`Flags packet`

`020104`

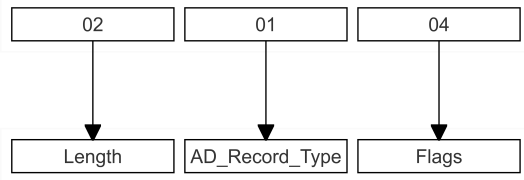

Figure 4: Advertising Data Part 2

2.3 Scan Response Data

The dongle scan response data includes:

- Full dongle name

Example dongle name `MUNIC_123456789012`

`Scan Response Data`

`13094D554E49435F31323334353637383930313 2`

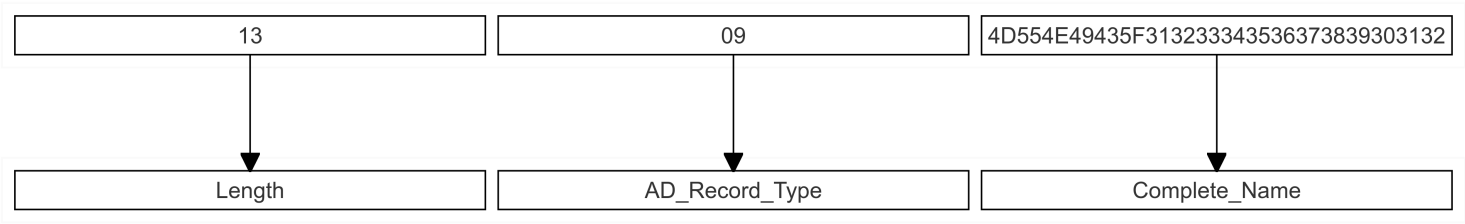

Figure 5: Scan Response Data

3 LE Connection

Once the phone application successfully locates the dongle through a Bluetooth Low Energy (BLE) scan, it initiates a connection request.

Upon establishing a connection, the phone app acts as a GATT client. This allows it to discover the services and characteristics offered by the dongle. By interacting with these characteristics, the phone app can exchange data with the dongle, such as sending authentication token.

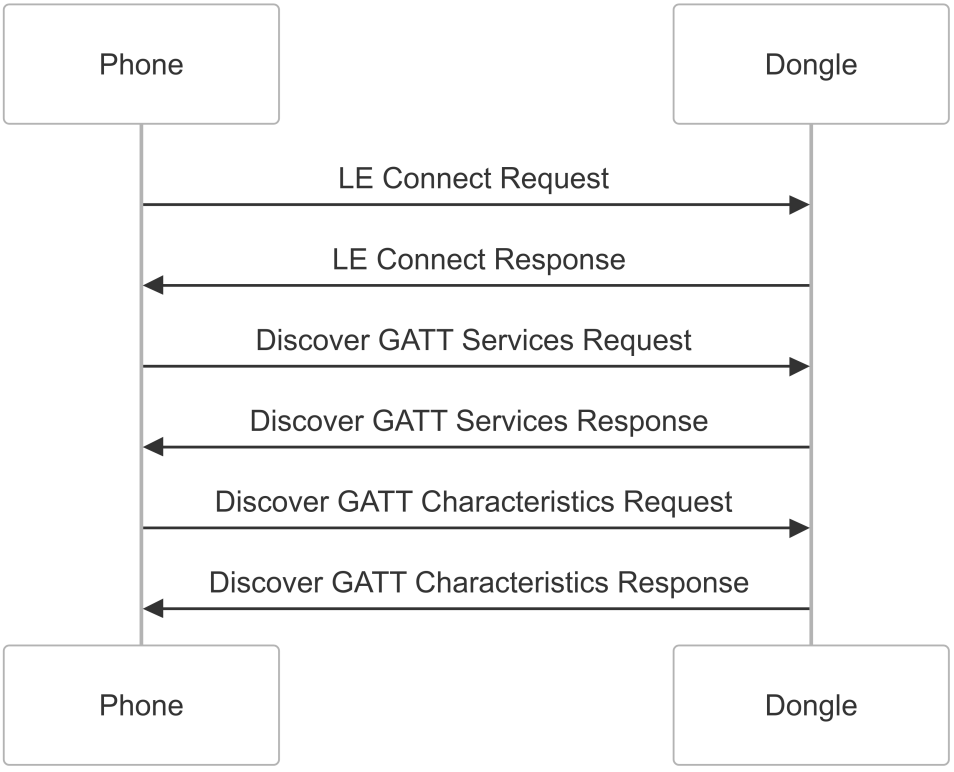

Figure 6: LE Connection

Once the phone app has discovered the necessary services and characteristics on the dongle, it can proceed to write data to specific characteristics.

To do this, the app sends a write characteristic value request to the dongle, specifying the target service UUID and characteristic UUID. Along with the request, the app includes the data to be written.

The dongle receives this request, writes the data to the designated characteristic, and sends a write characteristic value response to confirm the successful operation.

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

The service includes two characteristics. The first characteristic is used to write the authentication token, while the second characteristic is used to signal the completion of the token writing process and initiate the token validation procedure.

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

See Authentication Service document for more details.