Infineon Wi-Fi onboarding service (IWOS)

About this document

Scope and purpose

This document describes the Infineon Wi-Fi onboarding service that allows your device to transfer Wi-Fi credentials over a Bluetooth® LE link. It only describes the custom Bluetooth® LE GATT service and its behavior. The actual implementation is upto the user.

Intended audience

This document is primarily intended for anyone who want to use Infineon Wi-Fi onboarding service to onboard Wi-Fi using Bluetooth® LE.

Table of contents

Table of contents

1 Introduction

The Infineon Wi-Fi onboarding service allows a device to transfer Wi-Fi credentials over a Bluetooth® LE link. This service is defined over the GATT layer. This service exposes five characteristics for transferring Wi-Fi SSID, Wi-Fi password, Wi-Fi SSID and Password (together), Wi-Fi Networks, and control data.

1.1 Conformance

If a server claims conformance to any of the services, all capabilities indicated as mandatory for the service will be supported in the specified manner (process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated.

1.2 Service dependency

The services have no dependencies on other GATT-based services.

1.3 Transport dependencies

The services operate only over a Bluetooth® LE transport.

1.4 Byte transmission order

All characteristics used with these services are transmitted with the least significant octet first (i.e., little-endian).

2 Infineon Wi-Fi onboarding service definition

The IWO service is instantiated as a primary service with the service UUID set to the IWO service.

UUID	Value	Definition
IWO SERVICE	0x21C04D09-C884-4AF1-96A9-52E4E4BA195B	128-bit service UUID for Infineon Wi-Fi onboarding service

2.1 GATT sub-procedure requirements

The following additional GATT sub-procedures are required beyond those required by GATT:

GATT sub-procedure	Requirement (Optional/Mandatory)
Write characteristic value	O
Write without response	M
Read characteristic	O
Notification	M
Read characteristic descriptors	O
Write characteristic descriptors	O

2.2 Error codes

This service does not define any attribute protocol application error codes.

2.3 Characteristics overview

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

Characteristic name	Requirement	Properties	Format	UUID	Security permissions
WIFI SSID	C1	Read, write	String array (up to 32 bytes)	1E500043-6B31-4A3D-B91E-025F92CA9763	Read, write authentication required
WIFI PASSWORD	C1	Write	String array (up to 63 bytes)	1E500043-6B31-4A3D-B91E-025F92CA9764	Write authentication required
WIFI SSID PASSWORD	C1	Write	String array	1E500043-6B31-4A3D-B91E-025F92CA9765	Write authentication required
WIFI NETWORKS	M	Notify	String array	1E500043-6B31-4A3D-B91E-025F92CA9766	None
WIFI CONTROL	M	Write, notify	unsigned integer	1E500043-6B31-4A3D-B91E-025F92CA9767	Write authentication required

Note: Security permissions of “None” means that this service does not impose any requirements.

Either the **WIFI SSID PASSWORD** characteristic or **WIFI SSID** and **WIFI PASSWORD** characteristics are mandatory. All three can also be present at the same time.

2.4 WIFI SSID characteristic

The WIFI SSID characteristic is used to transmit the SSID of the Wi-Fi network that needs to be connected. The data has a variable length with the default size of 32 bytes. The server application receives the Wi-Fi SSID from the client device and stores it for future use when the connect command is issued by the client to connect to the specified Wi-Fi network.

2.4.1 Characteristic behavior

The server does not modify the data for this characteristic. Only the client can overwrite the data.

2.4.2 Characteristic descriptors

2.4.2.1 Characteristic user description

The *Characteristic User Description* descriptor is included in the WIFI SSID characteristic with the value **WiFi SSID**.

2.5 WIFI PASSWORD characteristic

The WIFI PASSWORD characteristic is used to transmit the password of the Wi-Fi network that needs to be connected. The data has a variable length with the default size of 63 bytes. The server application receives the Wi-Fi password from the client device and stores it for future use when the connect command is issued by the client to connect to the specified Wi-Fi network. This characteristic is write-only so that any random client cannot read the password.

2.5.1 Characteristic behavior

The server does not modify the data for this characteristic. Only the client can overwrite the data; the client cannot read the data.

2.5.2 Characteristic descriptors

2.5.2.1 Characteristic user description

The *Characteristic User Description* descriptor is included in the WIFI PASSWORD characteristic with the value **WiFi Password**.

2.6 WIFI SSID PASSWORD characteristic

The WIFI SSID PASSWORD characteristic is used to send the SSID and password data together, thus saving multiple writes. The data is formatted as type, length, value (TLV).

For SSID, the type value is ‘1’ and for password the type value is ‘2’. The first byte of the data should be type; for this example, it will be ‘1’ for SSID, followed by the length of the SSID, and then the SSID data (in hex format). This is followed by TLV value for password. For example: if the SSID is **WIFISSID** and password is **PASSWORD**, the formatted value will be:

01 08 57 49 46 49 53 53 49 44 02 08 50 41 53 53 57 4f 52 44

2.6.1 Characteristic behavior

The server does not modify the data for this characteristic. Only the client can overwrite the data; the client cannot read the data.

2.6.2 Characteristic descriptors

2.6.2.1 Characteristic user description

The *Characteristic User Description* descriptor is included in the WIFI SSID PASSWORD characteristic with the value **WiFi SSID** and **Password**.

2.7 WIFI NETWORKS characteristic

The WIFI SSID NETWORKS characteristic is used to send the nearby Wi-Fi networks to the client device.

The data is in the TLV format. The first byte indicates the type (**1** for SSID and **2** for security details). The next byte indicates the length of the data. After this data, there will be another type byte followed by the length and the data. The security value consists of four bytes (little-endian), which needs to be combined into a 32-bit value.

2.7.1 Characteristic behavior

The client cannot write to or read from this characteristic. Only the server can use this characteristic to send notifications to the client.

2.7.2 Characteristic descriptors

2.7.2.1 Characteristic user description

The *Characteristic User Description* descriptor is included in the WIFI NETWORKS characteristic with the value **WiFi Networks**.

2.8 WIFI CONTROL characteristic

The WIFI CONTROL characteristic is used by the client to send the disconnect (0), connect (1), and scan (2) commands to the server. It is also used by the server to notify the client whether the connection was successful.

2.8.1 Characteristic behavior

When the client writes ‘1’ to this characteristic, the server uses the data previously written to the WIFI SSID and WIFI PASSWORD characteristics or WIFI SSID PASSWORD characteristic to try and connect to the specified network. If no data is present, the server will notify the client with the ‘0’ value. Upon successful connection, the server will notify the client with the ‘1’ value. If connection is unsuccessful or a future disconnect, the server will notify the client with the ‘0’ value. To start scanning for Wi-Fi networks, the client needs to write the value ‘2’ to this characteristic.

2.8.2 Characteristic descriptors

2.8.2.1 Client characteristic configuration descriptor

The *Client Characteristic Configuration* descriptor is included in the WIFI CONTROL characteristic.

2.8.2.2 Characteristic user description

The *Characteristic User Description* descriptor is included in the WIFI Control characteristic with the value **WiFi Control**.

Revision history

Document version	Date of release	Description of changes
**	2021-08-13	Initial release
*A	2022-12-23	Replaced incorrect WIFI CONNECTION references to WIFI CONTROL

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2022-12-23

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Go to www.cypress.com/support

Document reference

002-33722 Rev. *A

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.