

ACTICORE1 Bluetooth Profile

Version: 1.4 (1st of July 2023)

Author: YB

Released by: DC

Introduction

The ACTICORE1 pelvic floor exercise device was designed to assist users in performing their pelvic floor exercises efficiently and comfortably. This innovative device technology combines state-of-the-art engineering with a user-friendly app to provide a comprehensive training experience.

The primary goal of the present Bluetooth profile for the ACTICORE1 pelvic floor exercise device is to enable manufacturers of other pelvic floor exercise devices to seamlessly integrate with the ACTICORE1-app. By implementing this profile, various manufacturers have the opportunity to synchronize their products with the proven ACTICORE1-app, thus benefiting from the advantages of a cutting-edge application.

This document describes the communication protocol between the ACTICORE1-Bluetooth sensors and the DiGA. It also explains the collected sensor data and its utilization.

Data

The ACTICORE1-application connects via Bluetooth to the ACTICORE1-Sensorseat. During the training session, the pressure sensor transmits a continuous stream of data to the ACTICORE1-application.

Persistence

The pressure sensor does not store any information; all data is directly transmitted via Bluetooth to the connected application. If the sensor is not connected to the application via Bluetooth, no data is stored on the sensor. At no point is any configuration saved on the sensor, and no personal data related to the patient is stored. Sensor data only holds health or personal significance when combined and processed within the application.

Profile

General workflow

This Bluetooth workflow encompasses device discovery, connection establishment, signature verification, data retrieval, and appropriate device handling to ensure a smooth and secure interaction with the Bluetooth device.

1. Discover the device:
 - a. Scan for nearby Bluetooth devices to discover the available devices.
 - b. If multiple devices are found, prompt the user to press the button on the desired device (again) for further identification. Select the device where the button-press-bit has toggled
2. Connect, discover services, and characteristics:
 - a. Establish a Bluetooth connection with the selected device.
 - b. Discover the supported services and characteristics provided by the device.
3. Subscribe to Signature ready (0x00000077):
 - a. Enable notifications for the Signature ready characteristic (0x00000077) to receive updates when the signature is ready for verification.
4. Generate random 16 bytes and write to Data to sign (0x00000074):
 - a. Generate a random 16-byte array and write it to the Data to sign characteristic (0x00000074) on the device. This data will be used for signature verification.
5. Wait for Signature ready to be 0x00000001:
 - a. Wait for the Signature ready characteristic to indicate that the signature generation process is complete (0x00000001). This may take up to 3 seconds.
6. Read Signature low (0x00000075) and Signature high (0x00000076):
 - a. Once the Signature ready characteristic is set to 0x00000001, read the Signature low (0x00000075) and Signature high (0x00000076) characteristics from the device.
 - b. Concatenate the two arrays to form a 256-byte long array for signature verification.
7. Check the signature for validity:
 - a. Use the provided public key to check the validity of the signature against the generated random bytes.
 - b. Hash the bytes using SHA256 (even with only 16 bytes) for signature verification.
 - c. If the signature check fails, prompt the user to abort or turn off the device.
8. Read auxiliary information:
 - a. Retrieve additional information as needed from relevant services, such as battery level from the Battery Service or version numbers from the Device Information Service.
9. Enable measurement value notifications (0x00000071):
 - a. If necessary, enable notifications for the Measurement value characteristic (0x00000071) to receive updates when new measurement values are available.

- b. Note that enabling these notifications may result in increased power consumption.
10. Disconnect or turn off the device
 - a. When the required tasks are completed, disconnect from the device or turn it off by writing `0x01` to the 'Turn off device characteristic' (`0xbb72`).

Advertising Packet

The advertising packet for the ACTICORE¹ Bluetooth device follows these specifications:

- ◇ General Discoverable: This device is set to be discoverable by other Bluetooth devices in the vicinity.
- ◇ BLE only: The device utilizes Bluetooth Low Energy (BLE) technology for efficient and power-saving communication. (`02 01 06`)
- ◇ Complete list of UUIDs: The device supports the Battery service, Device Info Service, and the Acticore Service. These services provide information about battery status, device information, and Acticore-specific functionalities. (`07 03 0f 18 0a 18 70 bb`)
- ◇ Complete local name: The device is identified by the name "ACTICORE" in the advertising packet. (`0a 09 41 63 74 69 63 6f 72 65 31`)
- ◇ Manufacturer data: The device includes manufacturer data indicating the state of the button being pressed. The specific data is represented as "Button Pressed State" and consists of four bytes: `04 ff ff ff 00`. The last byte, denoting the button state, will toggle between `0x00` and `0x01` with each button press.

Device Information Service (0x180a)

The Device Information Service of the Bluetooth profile provides essential information about the bluetooth device. The following characteristics are supported:

- ◇ Manufacture Name String (`0x2a29`):
 - ⇒ Characteristic Type: Read
 - ⇒ Returns the manufacture name of the device: Acticore
- ◇ Model Number String (`0x2a24`):
 - ⇒ Characteristic Type: Read
 - ⇒ Returns the model number or device name: Acticore1
- ◇ Hardware Revision String (`0x2a27`):
 - ⇒ Characteristic Type: Read
 - ⇒ Returns the PCB version number, which is printed on the overlay of the device. For example, it may return "1.5" indicating the PCB version.
- ◇ Firmware Revision String (`0x2a26`):
 - ⇒ Characteristic Type: Read

- ⇒ Returns the version number of the device's application firmware. For example, it may return "1.3.3" indicating the firmware version.
- ◇ Software Revision String (0x2a28):
 - ⇒ Characteristic Type: Read
 - ⇒ Returns the version number of the Silicon Labs Bluetooth Stack used by the device. For example, it may return "2.8.1.0" indicating the software revision.

Battery Service (0x180f)

The Battery Information Service, identified by the UUID 0x180f, is a default service provided by the Bluetooth SIG. It provides information about the battery level of the device. The following characteristic is supported:

- ◇ Battery Level (0x2a19):
 - ⇒ Characteristic Types: Read, Notify
 - ⇒ This characteristic provides the current battery level of the device in percentage. For example, it may indicate a battery level of "100%" when fully charged.

ACTICORE1 Service (0xbb70)

The ACTICORE1 Service, identified by the UUID 0xbb70, encompasses the main functionalities of the ACTICORE1 device, including weight/pressure measurement, device originality verification, and device control. It provides a comprehensive set of characteristics for weight/pressure measurement, device control, and verification purposes. With this service, users can monitor real-time measurements, initiate device turn-off, manage auto power off behavior, and perform signature generation and verification tasks to ensure the integrity and security of the ACTICORE1 device. The following characteristics are supported:

- ◇ Measurement Value (0xbb71):
 - ⇒ Characteristic Types: Read, Notify
 - ⇒ This characteristic provides the current pressure or weight measurement as an unsigned 16-bit integer. When notifications are enabled, new values are transmitted at a frequency of 20Hz. The values are filtered, centered within the 16-bit range, and adjusted to prevent toggling between 0x0000 and 0xffff.
- ◇ Turn Off Device (0xbb72):
 - ⇒ Characteristic Type: Write
 - ⇒ Writing the value 0x01 to this characteristic initiates an automatic disconnection and turns off the Acticore device. This action is equivalent to a button-short-press on the device.
- ◇ Button Pressed (0xbb73):

- ⇒ Characteristic Type: Read
- ⇒ This characteristic represents a toggling bit that changes upon each button-long-press of 3 seconds, alternating between the values `0x00` and `0x01`. Currently, this characteristic is not utilized as the same information is available in the advertising packet, which is used to determine the device to which the app should connect.
- ◇ Data to Sign (`0xbb74`):
 - ⇒ Characteristic Type: Write
 - ⇒ Users can write 16 bytes of random data to this characteristic, which will be signed using the private key (RSA-2048) for further verification purposes.
- ◇ Signature Low (`0xbb75`):
 - ⇒ Characteristic Type: Read
 - ⇒ This characteristic provides the lower 128 bytes of the generated signature.
- ◇ Signature High (`0xbb76`):
 - ⇒ Characteristic Type: Read
 - ⇒ This characteristic provides the higher 128 bytes of the generated signature.
- ◇ Signature Ready (`0xbb77`):
 - ⇒ Characteristic Types: Read, Notify
 - ⇒ The Signature Ready characteristic indicates whether a signature could be successfully generated and is ready to be read. The value `0x01` signifies that the signature is ready for retrieval.
- ◇ Auto Power Off Disable (`0xbb78`):
 - ⇒ Characteristic Type: Write
 - ⇒ Users can control the auto power off behavior of the Acticore device using this characteristic. By default, the device automatically turns off after 5 minutes of inactivity, either when disconnected or when connected with value notifications on but minimal changes in measured values. Writing the value `0x01` to this characteristic disables the auto power off feature, ensuring that the device only powers down when it has been disconnected for more than 5 minutes.