SGS01BTHome Manual

Document-Version: V1.0_rev_0

Operation

Die SGS01BTHome has two operation modes: “Connection Mode” and “Measure Mode”. On startup, if the device is not paired, it enters “Operation Mode” for 60 seconds, before switching to “Measure Mode”. If the device is already paired, it starts up directly with “Measure Mode”.

Connection Mode	Connect and pair the device. Unpaired device: Sends BLE ADVind advertisements with device name and appearance. Paired device: Sends BLE ADVdirect advertisements (no data). Mode timeout 60 seconds. BLE connection timeout 4 minutes.
Measure Mode	Config. Device Mode 0 (default, ultra low power): Sends BLE ADVnoconn advertisements with sensor data in BTHome format. Device is not connectable. ADV interval 8 seconds. Config. Device Mode 1: Sends BLE ADVind advertisements with sensor data in BTHome format and allows BLE connections “low duty”. ADV interval 3 seconds.

Button

Short Press	Toogle between the operation modes.
Long Press (10 sec)	Factory Reset (reset configuration. and pairing)

LED

The LED is connected to the MCU and cannot be controlled direct by the module firmware. The LED should flash in “Connection Mode”.

Encryption

To encrypt the device after a factory reset:

1. Connect (and pair) the device to get a BLE encrypted device connection.
2. Write a 6 digit pin number to the BLE attribute “Pin Code”.
   Format: 4 bytes little endian (eg. 0x40,0xE2,0x01,0x00 for “123456”).
3. Disconnect and reconnect/pair the device.
   For authentication enter the 6 digits pin number.
   An authenticated, encrypted and secured connection will be established.
   Rem.: May need delete pairing/bonding info at your BLE master before
   Rem.: Sometimes you need two attempts (Android, unknown reason)
4. The device will itself create and persist store a random CCM encryption key (16 bytes) for BTHome data.
   You can read and modify the key, see BLE attribute “Encryption Key”.
5. BTHome data will be send encrypted.

Alternative method “low-level” (No device connection or pairing needed):

1. After flashing the firmware – flash a configuration with a fixed encryption key.
2. Create a bin file with:
   4 bytes magic 68 61 70 70
   4 bytes zero
   16 bytes encryption key
   Example file is at “test/config-keytest.bin”.
3. Flash the configuration file to sector 7C000.
4. Restart the sensor with power off/on.

Sensor configuration

BLE Attribute	***Values***
“Pin Code”	6 digit number used for authentication. Value type: UINT32 little endian
“Encryption Key”	16 bytes value for BTHome data encryption (0=none)
“Power Level”	+10 to -5 dbm Value type: signed byte
“Device Mode”	0x00 = ultra low power (no connect in measure mode) 0x01 = medium power (connect in measure mode) see “Operation”
“Data Format”	0x00 = default (BTHome V2) 0x01 = BTHome V1 (depreciated, no encryption) 0x02 = BTHome V2 0x04 = Xiaomi (no encryption supported)
“Factory Reset”	0x02 = soft restart 0x03 = factory reset (Will be executed after disconnect)

Estimated battery lifetime

Current alive	3V 20mA (todo ? check/measure average)
Current deep sleep	3V 19uA
Critical Bat. Voltage	2,6V (2x 1,3V low duty)
Bat. Capacity:	1000 mAh
Dev.Mode 0: no conn	<4 ms / 8 sec (sleep/alive)
Dev.Mode 1: no conn	4,5 ms / 3 sec (sleep/alive)
Dev.Mode 2: conn	5 ms / 1 sec (sleep/alive)

Lifetime (calculated)

Dev.Mode 0: no conn	34800 hrs	**4 years**
Dev.Mode 1: no conn	20400 hrs	2,3 years
Dev.Mode 1: conn	8500 hrs	1 year

Remark: Values have to be checked.

BLE GATT attribute list

Service	1800	GAP
Device Name	2a00	
Appearance	2a01	
Peri.Conn.Param.	2a04	
Service	1801	GATT
Service Changed	2a05	
Service	180A	Device Information
Serial Number	2a25	
Firmware Revision	2a26	
Hardware Revision	2a27	
Software Revision	2a28	
Manufacturer	2a29	
Service	180F	Battery Service
Battery Level	2a19	
Service	DE8A5AAC-A99B-C315-0C80-60D4CBB51225	
Pin Code	0ffb7104-860c-49ae-8989-1f946d5f6c03	
Encryption Key	eb0fb41b-af4b-4724-a6f9-974f55aba81a	
Power Level	2a07	
Device Mode	9546a800-d32e-4573-81e1-d597c5e1da74	
Data Format	9546a801-d32e-4573-81e1-d597c5e1da74	
BTHome Data	d52246df-98ac-4d21-be1b-70d5f66a5ddb	
Factory Reset	b0a7e40f-2b87-49db-801c-eb3686a24bdb	
Service	00010203-0405-0607-0809-0a0b0c0d1912	TELink OTA
OTA Data	00010203-0405-0607-0809-0a0b0c0d2b12	

Copyright / Licence