



Table of Contents

Overview.....	1
BLE Advertisement.....	1
Advertisement Data.....	1
Scan Response Data.....	1
GATT Server.....	2
Custom Service.....	2
Custom Characteristics.....	2
Unlock.....	2
Date.....	3
Admin1.....	3
Admin2.....	3
UUID.....	4
Phone Number.....	4
History.....	4
Whitelist.....	5
Admin3.....	8
admin fields.....	9
External Interface.....	10
OTA Service.....	10
Device Control.....	10
Client Connection Protokoll.....	11
Notifications.....	11
Battery Update.....	11
Key Update.....	12
Lock Update.....	12
Unlock Lock.....	13
OTA Update.....	14
Initial State.....	14



Overview

BLE Advertisement

Currently the advertisement data is sent every second. If no device is asking for scan response data only the advertisement data will be sent. In the other cases there will also be the scan response data sent.

Advertisement Data

Byte	Value	Description
0	0x02	Length of next block in Byte
1	0x01	ad field type = Flags
2	0x06	Connectable/undirected
3	0x02	Length of next block in Byte
4	0x0A	Ad field type = TX Power
5	0xF3	TX power in dBm
6	0x18	Length of next block in Byte
7	0xFF	Ad field Type = Manufacturer Specific Data
8	0xFF	Prototype Company Identifier Code - octet 2
9	0xFF	Prototype Company Identifier Code - octet 1
10	0x00 – 0x64	Battery Percentage
11	0x00	Unused
12	0x00	Unused
13		Lockstate 0x0A unlocked else locked
14		Doorstate 0x02 door opened else closed
15		Lock mode
16	0x00-0xFF	Open time of Lock in normal mode
17 – 25		Firmware Version
26 – 30		Whitelist Version without Seconds

Scan Response Data

Byte	Value	Description
0	0x17	Length of next block in Byte
1	0x07	ad field type = Services 128 bit all
2 – 5	0x45523232	128bit for own Service
6 – 9	0x574F514B	



10 – 13	0x53434F2D	
14 – 17	0x4D4F4445	
18		Length of next block in Byte, Length of Lock name in Bytes
19-28		10 Bytes for Lock name
29 – 31	0x00	Unused

GATT Server

Custom Service

Service: 4d4f4445-5343-4f2d-574f-514b45523232

This Service is for the PS Locks BLE specific stuff.

Advertise True

Custom characteristics:

Name	Read/Write	Notify	UUID
Unlock	Write only	False	4d4f4445-5343-4f2d-574f-524a45523032
Date	Write only	False	4d4f4445-5343-4f2d-574f-524a45523033
Admin1	Write only	False	4d4f4445-5343-4f2d-574f-524a45523034
Admin2	Read/Write	False	4d4f4445-5343-4f2d-574f-524a45523035
UUID	Write only	False	4d4f4445-5343-4f2d-574f-524a45523036
Phone number	Write only	False	4d4f4445-5343-4f2d-574f-524a45523037
State notify	None	True	4d4f4445-5343-4f2d-574f-524a45523038
History	Read/Write	True	4d4f4445-5343-4f2d-574f-524a45523039
Whitelist	Read/Write	True	4d4f4445-5343-4f2d-574f-524a45523040
Admin3	Read/Write	False	4d4f4445-5343-4f2d-574f-524a45523041
Admin files	Read/Write	True	4d4f4445-5343-4f2d-574f-524a45523042
Ext. Interface	Write	False	4d4f4445-5343-4f2d-574f-514b45523001

Custom Characteristics

The following part describes, how data of the different characteristics are expected to send.

Unlock

Is used for unlocking lock. If mode is admin mode than lock is not opened or closed but its checked wether sent admin key is correct or not.

Byte	Description
0 - 5	Unlock key
6	Unlock mode



Unlock key must have 6 Byte. For 4 digit access key you have to add two '0'-characters (e.g.: 123400 for key 1234).

Mode	Description
0x31	UNLOCK_NORMAL Open lock for as many seconds as specified in admin2
0x32	UNLOCK_BOLT open lock continuously
0x33	UNLOCK_ADMIN

Date

Is used for history entry.

Byte	Description
0	Seconds
1	Minutes
2	Hour of day
3	Day of month
4	Month
5	Year % 100

Admin1

Admin Key has to be sent in the same session as the data is written or read.

With Admin1 the name of the lock can be changed.

Byte	Value	Description
0	0x02	Header for Lock name
1	0x00	Unused
2-11		Lock name (fill with 0's if length of name smaller than 10)

Admin2

Admin Key has to be sent in the same session as the data is written or read.

With Admin2 the access and admin key and the opening time in normal mode can be changed.

Byte	Description
0-3	Access key
4	Opening time in seconds



5	Opening time in seconds
6 – 11	Admin key
12-14	Desfire Application ID 3 bytes long
15	Desfire File ID 1 byte long
16-17	RFID reaction time in ms 2 bytes long

Desfire AID (15) and Desfire FID (16) are needed in case that Desfire Cards are used in gym or card cleaner mode. AID is a 3 byte number and FID one byte. For AID the number 0x000000 is not allowed as this is used for different purpose.

RFID reaction time is a two byte number which defines the time in ms between two card available checks.

When reading admin2 characteristic, access and admin key are set to zero due to security issues.

UUID

The UUID is used to give every user an unique ID for example on Android devices the ANDROID_ID can be used.

Byte	Description
0-9	Unique ID of User e.g. ANDROID_ID

Phone Number

The Phone number is used so that it's easy to see who opened the lock.

Byte	Description
0-9	Name/Nick Name/Phone Number/ or anything else

History

With History you can ask the lock for one history entry and history returns the entry.

Important is that there are saved the last 100 open/close lock actions. If all entries are full the oldest entries will be overwritten.

Write:

Byte	Description
0	Number of History Entry [0;99]; if Byte is 101 then number of history Entries



	is returned.
--	--------------

Read:

If the number of entries was requested:

Byte	Value	Description
0	0x65	101
1		Value between 0 and 99

If an entry was requested:

There will be sent 3 blocks of data. The first one includes the date, the second one the phone number or nick name and the third one the UUID.

Date Block:

Byte	Value	Description
0		Number of requested entry (between 0 and 99)
1	0x00	UPDATE_DATE
2 – 7		Date of requested Entry

Phone Block:

Byte	Value	Description
0		Number of requested entry (between 0 and 99)
1	0x01	UPDATE_PHONE OR_NAME
2 – 11		Phone number or name of requested Entry

UUID block:

Byte	Value	Description
0		Number of requested entry (between 0 and 99)
1	0x02	UPDATE_UUID
2 – 11		UUID of requested Entry

State Block:



Byte	Value	Description
0		Number of requested entry (between 0 and 99)
1	0x03	UPDATE_STATE_BLOCK
2		0x00 open lock / 0x01 close lock / 0x02 automatic close

Whitelist

The Whitelist is for saving the UID's of the cards which should have access to the lock.

Currently there are four possible commands on this characteristic:

Byte	Value	Description
0	0x00	Delete
0	0x01	Write
0	0x02	Read
0	0x03	Number of Entries
0	0x04	Whitelistversion

Whitelist delete

Send:

Byte	Value	Description
0	0x00	Delete

Response:

Byte	Value	Description
0	0x00	Delete
0	0x00	0x00/WHITELIST_DELETE_OK
	0x01	0x01/WHITELIST_DELETE_NOT_OK

Whitelist write entry Block

Send:

Byte	Value	Description
0	0x01	Write
1		Card ID length
2 - 8		Card ID



9 – 18		Name
19	0x00	0x00 disabled
	0x01	0x01 enabled
	0x02	0x02 programming card

Response:

Byte	Value	Description
0	0x01	Write
0	0x00	0x00/WHITELIST_WRITE_OK
	0x01	0x01/WHITELIST_WRITE_NOT_OK

Whitelist get number of entry block:

Send:

Byte	Value	Description
0	0x02	Read
1		Entry number

Response:

Byte	Value	Description
0	0x02	Read
1 – 4		Card ID
5 – 14		Name
15	0x00	0x00 disabled
	0x01	0x01 enabled

Whitelist get number of entry blocks:

Send:

Byte	Value	Description
0	0x03	Number of Entries

Response:



Byte	Value	Description
0	0x03	Number of Entries
1		Number of Entries

Whitelist Version block

Send:

Byte	Value	Description
0	0x04	Whitelistversion
1		Seconds
2		Minutes
3		Hour of day
4		Day of month
5		Month
6		Year % 100

Response:

Byte	Value	Description
0	0x04	Whitelistversion
1	0x00	0x00/WHITELIST_VERSION_OK
	0x01	0x01/WHITELIST_VERSION_NOT_OK

For creating a new Whitelist the steps have to be done in following order:

- Delete
- Write Version
- Write Entries

Admin3

Admin Key has to be sent in the same session as the data is written or read. When reading the value it is not necessary to send the admin key first. In iOS the reading is just done by the `peripheral.readValue(for:admin3Char)` call. If reading the data is finished you get a `didUpdateValueFor` call.

Byte	Value	Description
------	-------	-------------



0		Mode
1		Door open alarm 0 turned off else seconds until alarm starts
2		Reaction time in 0.1 second steps lower byte
3		Reaction time in 0.1 second steps upper byte
4		Open After
5		Sector 0 – 15
6		Block 0 – 2 if Sector is 0 only 1 – 2 is allowed
7 – 12		A-Key
13	0x00	0x00 RFID disabled
	0x01	0x01 RFID enabled
14	0x00	0x00 BLE disabled
	0x01	0x01 BLE enabled
15	0x00	0x00 Battery alarm disabled
	0x01	0x01 Battery alarm enabled
16	0x00	0x00 External Interface disabled
	0x01	0x01 External Interface enabled

Following modes are possible

Value	Mode
0x00	Normal Mode
0x01	GYM Mode
0x02	Card Cleaner
0x03	Learning Mode
0x04	Bolt Mode

Learning mode is for register new cards to the lock.

admin fields

Admin Key has to be sent in the same session as the data is written or read.

Byte	Value	Description
0		0x00 Write
		0x01 Read
1		Field
2-11		Data Value



Value and corresponding field number:

Value	Description
0	Lock name
1	Access Key
2	Admin Key
3	Opening time in seconds
4	Lock Mode (Card Cleaner, Normal, Gym...)
5	Door open alarm
6	Reaction time in 0. Second steps
7	Open after ... seconds
8	Sector 0-15
9	Block 0 – 2 if Sector is 0 only 1 – 2 is allowed
10	A-Key
11	RFID enable/disable
12	BLE enable/disable
13	Battery alarm enable/disable
14	External Interface enable/disable
15	Desfire Application ID 3 bytes long
16	Desfire File ID 1 byte long
17	RFID reaction time in ms 2 bytes long

Write Sector:

Byte	Value	Description
0	0x00	Write
1	0x08	Sector
2		Sector number

Read Sector:

Byte	Value	Description
0	0x00	Write
1	0x08	Sector

Response is in the same structure as write Sector.



External Interface

This interface is for opening and closing the lock.

Value	Description
0x01	Open the lock
0x02	Close the lock

OTA Service

Service: 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0

Characteristics for Update the firmware via OTA (over the air).

Value	Description
00737572-6573-686a-6f73-68692e636f6d	Ota data with response
01737572-6573-686a-6f73-68692e636f6d	Ota control without response

Device Control

Service: 00766963-6172-6173-6f6c-7574696f6e73

Characteristics for Update the firmware via OTA (over the air).

Value	Description
01766963-6172-6173-6f6c-7574696f6e73	Device reset

Client Connection Protokoll

For every operation the sequence should be:

- a. Detection and Connection
- b. Sending further commands (Read or Write)
- c. Receive any response if required
- d. Disconnection (Lock will disconnect automatically five seconds after last Read/Write action)

There can only connect one device per time to the lock.



Notifications

First Byte of Notification specifies the kind of Notification:

Value	Description
0x00	HANDLE_BATT_UPDATE
0x01	HANDLE_KEY_UPDATE
0x02	HANDLE_LOCK_UPDATE
0x03	HANDLE_ADMIN3_UPDATE
0x04	HANDLE_ADMIN_FIELD_UPDATE

Battery Update

Value	Description
0x00	Battery percentage [0;100]

Example:

Byte	Value	Description
0	0x00	HANDLE_BATT_UPDATE
1	0x09	9% of battery left

Key Update

Value	Description
0x00	KEY_NOT_OK
0x01	KEY_OK
0x02	Unused
0x03	KEY_BLOCKED after more than 3 wrong tries lock is blocked for 2 minutes
0x04	LOCK_WORKING if UNLOCK_NORMAL and open_time not yet expired

If KEY_BLOCKED a third byte is added, which contains the time the lock is blocked in minutes.

Examples:

Byte	Value	Description
0	0x01	HANDLE_KEY_UPDATE
1	0x01	KEY_OK



Example with three bytes:

Byte	Value	Description
0	0x01	HANDLE_KEY_UPDATE
1	0x03	KEY_BLOCKED
2	0x02	Lock is blocked for 2 minutes

Lock Update

Value	Description
0x00	LOCK_LOCKED
0x01	LOCK_UNLOCKED
0x02	LOCK_BOLTED
0x03	LOCK_ADMIN_NAME_WRITE
0x04	LOCK_ADMIN_KEYS_WRITE
0x05	DOOR_STATE

LOCK_ADMIN_NAME_WRITE and LOCK_ADMIN_KEYS_WRITE also contain a third byte:

Value	Description
0x00	LOCK_ADMIN_NAME_WRITE_SUCCESS
0x00	LOCK_ADMIN_KEYS_WRITE_SUCCESS
0x01	LOCK_ADMIN_NAME_WRITE_ERROR
0x01	LOCK_ADMIN_KEYS_WRITE_ERROR

Doorstate also contains a third byte describing the doorstate of the Lock:

Value	Description
0x02	Lock opened else closed

Examples:

Byte	Value	Description
0	0x01	HANDLE_LOCK_UPDATE
1	0x01	LOCK_UNLOCKED

Examples with three bytes:

Byte	Value	Description
0	0x02	HANDLE_LOCK_UPDATE



1	0x03	LOCK_ADMIN_NAME_WRITE
2	0x00	LOCK_ADMIN_NAME_WRITE_SUCCESS

Byte	Value	Description
0	0x02	HANDLE_LOCK_UPDATE
1	0x03	DOOR_STATE
2	0x02	Door opened

Admin3 Update

Value	Description
0x06	LOCK_ADMIN3_WRITE

LOCK_ADMIN3_WRITE also contain a third byte:

Value	Description
0x00	LOCK_ADMIN3_WRITE_SUCCESS
0x01	LOCK_ADMIN3_WRITE_ERROR

Example:

Byte	Value	Description
0	0x03	HANDLE_ADMIN3_UPDATE
1	0x06	LOCK_ADMIN3_WRITE
2	0x00	LOCK_ADMIN3_WRITE_SUCCESS

Unlock Lock

For unlocking the door following steps are recommended:

- Send date to lock
- Send Phone number to lock
- Send UUID to lock
- Send Unlock to lock

If these steps are executed then the history will be arranged correctly



If a wrong access or admin key is entered within a short time the lock will be blocked for two minutes and a notification will be sent.

OTA Update

The lock can be updated via Bluetooth which is called OTA (over the air).

For updating the firmware following steps are necessary:

- a. Send the admin key
- b. Send the data in blocks of 16 byte over the ota data with response characteristic
- c. Send the value 3 over the ota control without response characteristic

If these steps are executed then the update will work properly

Special Cards

Name	Value	Description
STD Group	0x5ea63deb	Sets all admin3 setting to default
Bold	0xdacf32e9	Activates bolt mode
Alarm	0xaeec3deb	Activates the door open alarm
Gym	0xf7a8333b	Activates gym mode
Gym_12	0x1e122acc	Activates gym mode and door open after 12h
Cleaner	0xf3e00100	Activates card cleaner mode
Bluetooth	0x140c0000	Allows to enable and disable bluetooth
Battery alarm	0x400f0000	Allows to enable and disable the battery alarm



API DUAL LOCK
Version: 06-08-2018

PS GmbH
Melisau 1255
6863 Egg / Austria
www.pslocks.com

Initial State

The lock has the same initial values as after resetting. They are all ASCII decoded:

Name: PSLOCK
Access Key: 1234
Admin Key: 123456

Settings:

Mode = Normal mode
Reaction time = 10
Door open alarm = OFF
Open After = 6
Sector = 4
Block = 1
A-Key = 0xFFFFFFFFFFFF
RFID = ON
BLE = ON
battery alarm = ON
external interface = OFF