Data Point Reference

Version: 20240314

Online Version

Contents

This topic describes the features, formats, and usages of data points (DPs) that apply to smart video locks.

1 Background

1.1 Terms

The following table lists the important terminologies that you may find helpful in understanding this topic. For more information, see Glossary.

Term	Explanation
Data point (DP)	A DP is an abstract representation of a feature you want to apply to a physical device, which can be defined by various data types.
Product ID (PID)	A PID is an abstract representation of a collection of physical devices that have the same configurations and properties. Each product created on the Tuya IoT Development Platform is assigned a unique PID that is associated with the product information, including DPs, app control panel, and purchase information.
Firmware key	The unique identity of firmware assigned by the Tuya IoT Development Platform.
Member	Also known as **user**.
Member ID	The ID of a member or a user, which is a 1-byte unsigned integer assigned and managed by the cloud. The valid values range from `0x01` to `0x64`. The rest are reserved.

Term	Explanation
Hardware ID	The ID of the hardware specific to an unlocking method, which is a 1-byte unsigned integer assigned and managed by the local processor. The valid values range from `0x00` to `0xFE`. `0xFF` is reserved. For example, for fingerprint unlocking and password unlocking, the hardware ID is `0x01` and `0x02` respectively.
Validity period	A specific unlocking method (such as fingerprint, password, and door card) is valid during the specified time period.
Cloud-to-device messaging	Data is sent from a mobile phone to a device.
Device-to-cloud messaging	Data is sent from a device to a mobile phone.

1.2 DP format

The size of `dp_data_len` is two bytes for smart video locks. The following table details the DP format.

Field

Bytes

Description

dp_id

1

The ID of a DP.

dp_type

1

The data type of a DP.

dp_data_len

2

The data length of a DP.

dp_data_value

dp_data_len

The payload of a DP.

2 Manage unlocking methods

2.1 Add unlocking methods

Data
transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

1

Raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(1 byte)

Hardware ID
(1 byte)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

Message UUID
(2 bytes)

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00:
Start enrollment.
0xFE:
Cancel enrollment (
initiated by app).

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

See Appendix: Validity period.

0x00: Permanent
0x01: One-time
…
0xFE: 254 times
0xFF: Expired

The bytes of a password
(used for unlocking with password only)

The password is sent in the numerical format. The valid values for each byte range from 0x00 to 0x09.

For example, if a password is 123456, the data to be sent is

[0x01,0x02,0x03,0x04,0x05,0x06]

When the password length is 0, the field of password content is not passed in.

Description

Device-to-cloud

1

Raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(1 byte)

Hardware ID
(1 byte)

Number of times
(1 byte)

Return value
(1 byte)

Message UUID
(2 bytes)

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00:
Start enrollment.

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

The number of times to finish enrollment
For example, six to eight times for fingerprint enrollment. One time for door card or face enrollment.

0x00: Default value

Same as above.

0xFC:
Enrollment in progress

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

The sequence number for enrollment times, starting from 1. For example, fingerprint enrollment might be eight times.
This field is populated with the current times.

Reasons for failed enrollment:
0x00: Success.
0x01: Fingerprint-scanning failed due to incomplete fingerprint or a wet finger.

0xFD:
Enrollment failed.

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

Current enrollment stage:
0x00: Start enrollment.
0xFC: Enrollment in progress.
0xFF: Finish enrollment.

Reasons for failed enrollment

0xFE:
Cancel enrollment (
initiated by app).

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

0x00: Default value

0x00: Default value

0xFF:
Enrollment is finished.

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

Hardware ID assigned to the device.
Valid values range from 0x00 to 0xFE.

0x00: Default value

0x00: Default value

Interaction example

- The following figure shows how the mobile app interacts with the lock during the enrollment of the password, door card, and face.
- The following figure shows how the mobile app interacts with the lock during the fingerprint enrollment.

2.2 Delete unlocking methods

Data
transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

2

Raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(1 byte)

Hardware ID
(1 byte)

Deletion method
(1 byte)

0x00: Delete a member.

0x00: Default

0x00: Default
The MCU does not need to check this field.

0x01 to 0x64

0xFF: Default value

0x00: Delete all the unlock methods granted to a member.

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0x00 to 0xFE

0x01: Delete a specified unlocking method granted to a member.

Device-to-cloud

2

Raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(1 byte)

Hardware ID
(1 byte)

Deletion method
(1 byte)

Return value
(1 byte)

0x00: Delete a member.

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

0x00: Delete all the unlock methods granted to a member.

0x00: Deletion failed.
0xFF: Deletion succeeded.
0x01: Hardware ID does not exist.
0x02: Hardware ID cannot be deleted, such as the hardware ID associated with the admin.

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0x00 to 0xFE

0x01: Delete a specified unlocking method granted to a member.

0x00: Deletion failed.
0xFF: Deletion succeeded.
0x01: Hardware ID does not exist.
0x02: Hardware ID cannot be deleted, such as the hardware ID associated with the admin.

2.3 Modify unlocking methods

Data
transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

3

Raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(1 byte)

Hardware ID
(1 byte)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

0x00: Modify the validity period for members.

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

See
Appendix: Validity period.

0x00: Default value.
(Modification is not allowed)

The bytes of a password
(used for unlocking with password only)

Description

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0x00 to 0xFE

See
Appendix: Validity period.

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

The bytes of a password
(used for unlocking with password only)

Same as above.

Device-to-cloud

3

Raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(1 byte)

Hardware ID
(1 byte)

Number of times
(1 byte)

Return value
(1 byte)

0x00:
Modify the validity period for a specified member.

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0xFF: Default value

0x00: Default value.
(Modification is not allowed)

0x00: Failure
0xFF: Success

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x01 to 0x64

0x00 to 0xFE

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

0x00: Failure
0xFF: Success

3 Manage temporary passwords

3.1 Add temporary passwords

The types of temporary passwords include one-time and recurring. The temporary password is different from the ordinary password in the following ways:

- A temporary password is not associated with any members.
- The validity period of a temporary password can be modified when the lock is connected.
- As an unlocking method, the type of the temporary password is defined as `0xF0`. `0x01` indicates password. `0x02` indicates door card. `0x03` indicates fingerprint.
- When responding to the cloud, the lock must report the hardware ID together with the cloud-preassigned temporary password ID to sync the mapping relationship between the two IDs with the cloud.

Take care of the following possible **issue** with temporary passwords:

- If the lock fails to sync the internal clock with the server time due to a power failure, this can cause the schedule for recurring access to not work properly.
- Solution:
  - Add a backup battery to the lock to ensure it can still be connected to the cloud even after a power failure.
  - You can accept the problems that might arise.

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

4

Raw

len

Cloud-assigned ID
(2 bytes)

State (1 byte)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

An associated ID assigned by the cloud.

0x00: Invalid
0x01: Valid

See Appendix: Validity period.

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

The bytes of a password
(used for unlocking with password only)

Same as Add Unlocking Methods.

Device-to-cloud

4

Raw

len

Cloud-assigned ID
(2 bytes)

Hardware ID
(1 byte)

Return value
(1 byte)

Same as above.

0x00 to 0xFE

0x00: Success.
0x01: Failure
0x02: Hardware ID is assigned.

3.2 Delete temporary passwords

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

5

Raw

len

Hardware ID
(1 byte)

0x00 to 0xFE

Device-to-cloud

5

Raw

len

Hardware ID
(1 byte)

Return value
(1 byte)

0x00 to 0xFE

0x00: Success.
0x01: Failure.

3.3 Modify temporary passwords

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

6

Raw

len

Hardware ID
(1 byte)

State (1 byte)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

0x00 to 0xFE

0x00: Invalid
0x01: Valid

See Appendix: Validity period.

Same as Adding Temporary Passwords.

The bytes of a password
(used for unlocking with password only)

```
1  <td align="left" nowrap>Same as Adding Temporary Passwords.<br>
```

Device-to-cloud

6

Raw

len

Hardware ID
(1 byte)

Return value
(1 byte)

0x00 to 0xFE

0x00: Success.
0x01: Failure.

4 Sync unlocking methods

- **Purpose**: To ensure the unlocking methods in the local device and the server are in sync, each time users open the lock member list or pull down to refresh the list, all the added unlocking methods will be synced between them.
- **Hardware types**: Used to notify the lock of what unlocking methods it should report. For the **in-sync** stage, the data length of each packet is defined by you. The total length of one packet should not exceed 200 bytes.
- **Sync locally-added unlocking methods**: A lock syncs the locally-added unlocking methods with the cloud in the following cases:
  - If the member ID is `0xFF`, the cloud saves this ID and associates the reported unlocking method with the app account that is bound with this lock. The member ID `0xFF` is used when the cloud sends commands of this unlocking method. Note that this member ID cannot be deleted from the cloud.
  - If the member ID is `0xFD`, the cloud saves this ID and associates the reported unlocking method with the app account that is bound with this lock. The member ID `0xFD` is used when the cloud sends commands of this unlocking method. Note that this member ID is generic.

  :::important
  This solution allows users to create temporary passwords that can be used when the lock gets offline. These passwords are cached in the cloud. After the lock gets back online and downloads the cached temporary passwords from the cloud, it should proactively sync the mapping relationship between the cloud-assigned ID and the hardware ID.
  :::

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

7

Raw

len

Hardware types
(len bytes)

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein
0xF0: Temporary password

Device-to-cloud

7

Raw

len

Stage
(1 byte)

Packet sequence number
(1 byte)

Data for sync
(n bytes)

0x00: In-sync

0x00 to 0xFF
The packet sequence number starts from 0, incrementally in order.

Data 1, Data 2 ⋯Data n

Data format definition

Device-to-cloud

7

Raw

len

Stage
(1 byte)

Total packets
(1 byte)

0x01: Sync finished

Total packets
For example, if a packet for the in-sync stage is delivered twice, the packets are two in total.

5 Manage remote unlocking

5.1 Set a key

- A key is required to use remote unlocking. The cloud sends the key to the lock after successful pairing. The MCU can also request the key.
- The **key** for **remote unlocking (DP 10)** is configured through **the command for setting keys**.
- In this command, **validity**, **member ID**, **start time**, **end time**, and **access times** are reserved fields.

  :::important
  To enhance security, the key for remote unlocking is updated occasionally. The cloud determines the update rule. After a key is used for `n` times, the cloud sends a new key to the lock through DP 9.
  :::

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

9

Raw

len

Validity
(1 byte)

Member ID
(2 bytes)

Start time
(4 bytes)

End time
(4 bytes)

Access times
(2 bytes)

Key
(8 bytes)

0x00: Invalid
0x01: Valid

0x01 to 0x64

Unix timestamp

Unix timestamp

0x0000 to 0xFFFF

ASCII code

Device-to-cloud

9

Raw

len

Return value
(1 byte)

Member ID
(2 bytes)

0x00: Success.
0x01: Failure.
0x10: Request for the remote unlocking key.

We recommend the MCU record the state of acquiring the key. If the key is not acquired, the module requests the key each time it is connected to the cloud.

0x01 to 0x64

5.2 Remote unlocking

Remote unlocking indicates the door is unlocked through non-short-range communication such as Bluetooth, which applies to Wi-Fi smart video locks.

- If the command is initiated by a mobile app, this is called **remote unlocking by app**.
- If the command is initiated by a smart speaker, this is called **remote unlocking by voice**.

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

10

Raw

len

State (1 byte)

Member ID
(2 bytes)

Key
(8 bytes)

Unlocking methods
(2 bytes)

0x00: Lock.
0x01: Unlock.

0x01 to 0x64

ASCII code

0x0000: Remote unlocking by unknown methods.
0x0001: Remote unlocking by app. 0x0002:
Remote unlocking by voice.

Device-to-cloud

10

Raw

len

Return value
(1 byte)

Member ID
(2 bytes)

0x00: Success.
0x01: Failure.
0x02: The key is invalid.
0x03: The access times run out.
0x04: The current time is not in the validity period.
0x05: Key comparison does not pass.

0x01 to 0x64

6 Lock settings

Feature

Messaging direction

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value
(len bytes)

Doorbell ringtones

Cloud-to-device/device-to-cloud

20

enum

0x01

Ringtones (1 byte)

0x00: Ringtone 0
0x01: Ringtone 1
...
0x0A: Ringtone 10

Doorbell volume

Cloud-to-device/device-to-cloud

21

enum

0x01

Volume (1 byte)

0x00: Mute

0x01: Low volume

0x02: Medium volume

0x03: High volume

System language

Cloud-to-device/device-to-cloud

22

enum

0x01

Languages (1 byte)

0x00: Simplified Chinese

0x01: English

0x02: Japanese

0x03: German

0x04: Spanish

0x05: Latin

0x06: French

0x07: Russian

0x08: Italian

0x09: Traditional Chinese

0x0A: Korean

Auto-locking settings

Cloud-to-device/device-to-cloud

23

bool

0x01

State (1 byte)

0x00: Turn off.
0x01: Turn on.

Delay for auto-locking

Cloud-to-device/device-to-cloud

24

value

0x04

The length of time delay (4 bytes)

0x00000001 to 0xFFFFFFFF
in seconds

Single/combined unlocking

Cloud-to-device/device-to-cloud

25

enum

0x01

Combined unlocking methods (1 byte)

0x00: Unlock with a single method

0x01: Fingerprint + Password

0x02: Fingerprint + Door card

0x03: Fingerprint + Face

0x04: Password + Door card

0x05: Password + Face

0x06: Door card + Face

Turn on/off locking check

Cloud-to-device/device-to-cloud

26

bool

0x01

State (1 byte)

0x00: Turn off.
0x01: Turn on.

Arm away

Cloud-to-device/device-to-cloud

27

bool

0x01

State (1 byte)

0x00: Turn off.
0x01: Turn on.

Do not disturb (DND)

Cloud-to-device/device-to-cloud

28

bool

0x01

State (1 byte)

0x00: Turn off.
0x01: Turn on.

DND period

Cloud-to-device/device-to-cloud

29

raw

0x04

Start time
(2 bytes)

End time
(2 bytes)

HH:MM
(hour:minute)

HH:MM
(hour:minute)

Keep-alive on/off

Cloud-to-device/device-to-cloud

44

bool

0x01

State (1 byte)

0x00: Off (non-keep-alive). Wi-Fi goes online as needed.
0x01: On (keep-alive). Wi-Fi stays online and enters sleep mode at the specified time.
DP 44 and DP 30 are mutually exclusive. If both DPs are selected, DP 44 takes precedence.

Sleep mode

Cloud-to-device/device-to-cloud

30

bool

0x01

State (1 byte)

0x00: Off.
0x01: On.
DP 44 and DP 30 are mutually exclusive. You can choose either.

Sleep mode time period

Cloud-to-device/device-to-cloud

31

raw

0x05

Start time
(2 bytes)

End time
(2 bytes)

Weekly schedule
(1 byte)

HH:MM
(hour:minute)

HH:MM
(hour:minute)

0x00: One-time

See Appendix: Validity period

User guide

Cloud-to-device/device-to-cloud

32

raw

0x02

Feature (1 byte)

State (1 byte)

0x00: Angle
0x01: Hover
...

0x00: Success.
0x01: Failure.

Special control

Cloud-to-device/device-to-cloud

33

bool

0x01

State (1 byte)

0x00: Turn off.
0x01: Turn on.

Special features

Cloud-to-device/device-to-cloud

34

enum

0x01

Custom features (1 byte)

0x00: Feature 0
0x01: Feature 1
…

Electronic double locking

Cloud-to-device/device-to-cloud

35

bool

0x01

State (1 byte)

0x00: Turn off.
0x01: Turn on (only the admin can unlock the door).

Manual locking

Cloud-to-device

8

bool

0x01

Fixed value (1 byte)

0x01

```
<td align="left" nowrap rowspan="2">Device-to-cloud</td>
<td align="left" nowrap rowspan="2">8</td>
<td align="left" nowrap rowspan="2">bool</td>
<td align="left" nowrap rowspan="2">0x01</td>
<th align="left" nowrap colspan="3">Return value (1 byte)</th>
```

0x00: Failure.
0x01: Success.

7 Report real-time status

Feature

Messaging direction

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value
(len bytes)

Operating state

Device-to-cloud

11

enum

0x01

Mode (1 byte)

0x00: keep_alive
0x01: sleep
0x02: lock_keep
0x03: lock_sleep

Alkaline battery level

Device-to-cloud

45

Value

0x04

Battery level (4 bytes)

0x00 to 0x64

Lithium-ion battery level

Device-to-cloud

46

Raw

0x02

Battery level (1 byte)

Charging state (1 byte)

0x00 to 0x64: Battery level
0xFF: Failed to obtain the battery level

0x00: Not charged

0x01: Charging

0x02: Fully charged

Locking/unlocking state

Device-to-cloud

47

Boolean

0x01

State (1 byte)

0x00: Locked
0x01: Unlocked

Child lock

Device-to-cloud

48

Boolean

0x01

State (1 byte)

0x00: Turn off the child lock.
0x01: Turn on the child lock.

Lift-up double locking

Device-to-cloud

49

Boolean

0x01

State (1 byte)

0x00: Not double locked by lifting up the handle
0x01: Double locked by lifting up the handle

Double locking state

Cloud-to-device/device-to-cloud

50

Boolean

0x01

State (1 byte)

0x00: Not double locked
0x01: Double locked

Door open/closed state

Device-to-cloud

51

enum

0x01

State (1 byte)

0x00: The door is closed
0x01: The door is open
0x02: Unknown
Note: The definitions of enumeration values are different from other all-in-one versions

Unlock from inside

Device-to-cloud

52

Boolean

0x01

State (1 byte)

0x00: Undefined
0x01: Unlock from inside

8 Report records

8.1 Alert and unlocking records

Feature

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(1 byte)

dp_data_value
(len bytes)

Doorbell records

Device-to-cloud

53

Boolean

0x01

State (1 byte)

0x00: Undefined
0x01: Calling

Alert records

Device-to-cloud

60

enum

0x01

Reasons for alerts (1 byte)

Value range

Ordinary password unlocking records

Device-to-cloud

61

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Fingerprint unlocking records

Device-to-cloud

63

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Door card unlocking records

Device-to-cloud

64

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Face unlocking records

Device-to-cloud

65

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Palm print unlocking records

Device-to-cloud

66

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Finger vein unlocking records

Device-to-cloud

67

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Iris unlocking records

Device-to-cloud

68

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Temporary password unlocking

Device-to-cloud

69

Value

0x04

Hardware ID (4 bytes)

0x00 to 0xFE

Mechanical key unlocking

Device-to-cloud

71

Value

0x04

Invalid field (4 bytes)

Populated with 0xFF

Remote unlocking by app

Device-to-cloud

72

Value

0x04

Member ID (4 bytes)

0x01 to 0x64

Remote unlocking by voice

Device-to-cloud

73

Value

0x04

Member ID (4 bytes)

0x01 to 0x64

8.2 Locking records

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Device-to-cloud

62

Raw

0x05

Locking methods
(1 byte)

Member ID
(4 bytes)

0x00: Locking by undefined methods
0x01: Remote locking by app
0x02: Remote locking by voice
0x03: Geofencing-based locking
0x04: Locking by app
0x05: Locking by using accessory
0x06: Auto-locking
0x07: Manual locking

0x01 to 0x64

8.3 Combined unlocking records

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Device-to-cloud

70

Raw

len

Combined unlocking methods
(1 byte)

Unlocking method 1
(1 byte)

Hardware ID 1
(1 byte)

Unlocking method 2
(1 byte)

Hardware ID 2
(1 byte)

0x01: Fingerprint + Password
0x02: Fingerprint + Door card
0x03: Fingerprint + Face
0x04: Password + Door card
0x05: Password + Face
0x06: Door card + Face

```
<td align="left" nowrap>
    0x01: Password <br>0x02: Door card <br>0x03: Fingerprint <br>0x04:
       Face <br>0x05: Palm print <br>0x06: Finger vein <br>0xF0:
       Temporary password</th>
<td align="left" nowrap>0x01 to 0xFE</td>
<td align="left" nowrap>Same as unlocking method 1</th>
<td align="left" nowrap>0x01 to 0xFE</td>
```

9 Offline password

- **Scenarios:**

  The door lock user gets an offline password from the app and notifies the visitor of this password. The offline password can be the following types:

  - One-time password: It is valid for six hours and can be used only once. If the password is used within the validity period, an unlocking record is created.
  - Timed password: It must be used once within 24 hours for activation. Otherwise, it will expire. It can be used unlimited times within the specified validity period. Every unlocking operation is recorded.
  - The code to clear a single password: It has the same validity period as the corresponding password and takes effect only on the first-time usage. A record of **clearing a single password** is created after the code is used.
  - The code to clear all passwords: It is a one-time clear code and valid for 24 hours. A record of clearing all passwords is created after the code is used.

- **Limitations on clearing a single password or all passwords:**

  - Only the **activated and valid password** can be cleared.
  - The **one-time password** cannot be cleared because it is invalid after use.

- **Usage**: For more information, see Serial Communication Protocol.

Feature

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(1 byte)

dp_data_value

Offline password
Set T0 time

Cloud-to-device/device-to-cloud

86

String

len

T0 timestamp (10 bytes)

Unix timestamp
The module processes this DP, without the MCU taking care of it.

Offline password
unlocking records

Device-to-cloud

89

Raw

0x10

Encrypted password (16 bytes)

For more information, see Serial Communication Protocol.

Offline password
Clear a single record

Device-to-cloud

87

Raw

0x10

The encrypted code for clearing passwords (16 bytes)

For more information, see Serial Communication Protocol.

Offline password
Clear all records

Device-to-cloud

88

Raw

0x10

The encrypted code for clearing passwords (16 bytes)

For more information, see Serial Communication Protocol.

10 Manage unlocking methods (bulk version)

Background: The default or standard solution supports only a 1-byte member and unlocking method, which is insufficient for access control devices. To address this limitation, a new set of bulk version DPs is designed to manage large-sized members and unlocking methods. The bulk version DPs **differ from the standard version DPs only in the bytes of member ID and hardware ID**. When you create products or write code, select the DP of the required version.

10.1 DP ID mapping

DP	Default/standard version	Bulk version
Add unlocking methods	DP ID=1	DP ID=13
Delete unlocking methods	DP ID=2	DP ID=14
Modify unlocking methods	DP ID=3	DP ID=15
Add temporary passwords	DP ID=4	DP ID=16
Delete temporary passwords	DP ID=5	DP ID=17
Modify temporary passwords	DP ID=6	DP ID=18
Sync unlocking methods	DP ID=7	DP ID=19
Combined unlocking records	DP ID=70	DP ID=74

10.2 Add unlocking methods

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

13

raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(2 bytes)

Hardware ID
(2 bytes)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

Message UUID
(2 bytes)

0x01: Password
0x02: Door card
0x03: Fingerprint

0x04: Face
0x05: Palm print
0x06: Finger vein

0x00:
Start enrollment.
0xFE:
Cancel enrollment
(initiated by app).

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0xFFFF: Default value

See Appendix: Validity period.

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

The bytes of a password
(used for unlocking with password only)

The password is sent in the numerical format. The valid values for each byte range from 0x00 to 0x09.

For example, if a password is 123456, the data to be sent is

[0x01,0x02,0x03,0x04,0x05,0x06]

When the password length is 0, the field of password content is not passed in.

Description

Device-to-cloud

13

raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(2 bytes)

Hardware ID
(2 bytes)

Number of times
(1 byte)

Return value
(1 byte)

Message UUID
(2 bytes)

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00:
Start enrollment.

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0xFFFF: Default value

The number of times to finish enrollment
For example, six to eight times for fingerprint enrollment. One time for door card or face enrollment.

0x00: Default value

Same as above.

0xFC:
Enrollment in progress

0x00: Ordinary member
0x01: Admin

Same as above.

Same as above.

The sequence number for enrollment times, starting from 1.
For example, fingerprint enrollment might be eight times. This field is populated with the current times.

Reasons for failed enrollment:
0x00: Success.
0x01: Fingerprint-scanning failed due to incomplete fingerprint or a wet finger.

0xFD:
Enrollment failed

0x00: Ordinary member
0x01: Admin

Same as above.

Same as above.

Current enrollment stage:
0x00: Start enrollment.
0xFC: Enrollment in progress.
0xFF: Finish enrollment.

Reasons for failed enrollment

0xFE:
Cancel enrollment
(initiated by app).

0x00: Ordinary member
0x01: Admin

Same as above.

Same as above.

0x00: Default value

0x00: Default value

0xFF:
Enrollment is finished.

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

Hardware ID assigned to the device.
Valid values range from 0x0000 to 0xFFFE.

0x00: Default value

0x00: Default value

10.3 Delete unlocking methods

Data
transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

14

raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(2 bytes)

Hardware ID
(2 bytes)

Deletion method
(1 byte)

0x00: Delete a member.

0x00: Default

0x00: Default
The MCU does not need to check this field.

0x0001 to 0xFFFF

0xFFFF: Default value

0x00: Delete all the unlock methods granted to a member.

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0x0000 to 0xFFFE

0x01: Delete a specified unlocking method granted to a member.

Device-to-cloud

14

raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(2 bytes)

Hardware ID
(2 bytes)

Deletion method
(1 byte)

Return value
(1 byte)

0x00: Delete a member.

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0xFFFF: Default value

0x00: Delete all the unlock methods granted to a member.

0x00: Deletion failed.
0xFF: Deletion succeeded.
0x01: Hardware ID does not exist.
0x02: Hardware ID cannot be deleted, such as the hardware ID associated with the admin.

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0x0000 to 0xFFFE

0x01: Delete a specified unlocking method granted to a member.

0x00: Deletion failed.
0xFF: Deletion succeeded.
0x01: Hardware ID does not exist.
0x02: Hardware ID cannot be deleted, such as the hardware ID associated with the admin.

10.4 Modify unlocking methods

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

15

raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(2 bytes)

Hardware ID
(2 bytes)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

0x00: Modify the validity period for members.

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0xFFFF: Default value

See
Appendix: Validity period.

0x00: Default value.
(Modification is not allowed)

The bytes of a password
(used for unlocking with password only)

Description

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0x0000 to 0xFFFE

See
Appendix: Validity period.

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

The bytes of a password
(used for unlocking with password only)

Same as above.

Device-to-cloud

15

raw

len

Type
(1 byte)

Stage
(1 byte)

Admin flag
(1 byte)

Member ID
(2 bytes)

Hardware ID
(2 bytes)

Number of times
(1 byte)

Return value
(1 byte)

0x00: Modify the validity period
for a specified member.

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0xFFFF: Default value

0x00: Default value.
(Modification is not allowed)

0x00: Failure
0xFF: Success

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

0x00: Default

0x00: Ordinary member
0x01: Admin

0x0001 to 0xFFFF

0x0000 to 0xFFFE

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

0x00: Failure
0xFF: Success

10.5 Add temporary passwords

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

16

raw

len

Cloud-assigned ID
(2 bytes)

State
(1 byte)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

An associated ID assigned
by the cloud.

0x00: Invalid
0x01: Valid

See Appendix: Validity period.

0x00: Permanent
0x01: One-time
...
0xFE: 254 times
0xFF: Expired

The bytes of a password
(used for unlocking with password only)

Same as Add
Unlocking Methods.

Device-to-cloud

16

raw

len

Cloud-assigned ID
(2 bytes)

Hardware ID
(2 bytes)

Return value
(1 byte)

Same as above.

0x0000 to 0xFFFE

0x00: Success.
0x01: Failure
0x02: Hardware ID is assigned.

10.6 Delete temporary passwords

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

17

raw

len

Hardware ID
(2 bytes)

0x0000 to 0xFFFE

Device-to-cloud

17

raw

len

Hardware ID
(2 bytes)

Return value
(1 byte)

0x0000 to 0xFFFE

0x00: Success.
0x01: Failure.

10.7 Modify temporary passwords

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

18

raw

len

Hardware ID
(2 bytes)

State
(1 byte)

Validity period
(17 bytes)

Number of times
(1 byte)

Password length
(1 byte)

Password content
(n bytes)

0x0000 to 0xFFFE

0x00: Invalid
0x01: Valid

See Appendix: Validity period.

Same as Adding
Temporary Passwords.

The bytes of a password
(used for unlocking with password only)

```
<td align="left" nowrap>Same as Adding <br>Temporary Passwords.
```

Device-to-cloud

18

raw

len

Hardware ID
(2 bytes)

Return value
(1 byte)

0x0000 to 0xFFFE

0x00: Success.
0x01: Failure.

10.8 Sync unlocking methods

This solution allows users to create temporary passwords that can be used when the lock gets offline. These passwords are cached in the cloud. After the lock gets back online and downloads the cached temporary passwords from the cloud, it should proactively sync the mapping relationship between the cloud-assigned ID and the hardware ID.
The device proactively reports temporary passwords, while the cloud does not issue a temporary password sync command. Therefore, the message ID is fixed as `0xFFFF`.

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Cloud-to-device

19

raw

len

Message ID
(2 bytes)

Hardware types
(n bytes)

Used to be associated
with a packet

0x01: Password
0x02: Door card
0x03: Fingerprint
0x04: Face
0x05: Palm print
0x06: Finger vein

Device-to-cloud

19

raw

len

Stage
(1 byte)

Message ID
(2 bytes)

Packet sequence number
(1 byte)

Data for sync
(n bytes)

0x00: In-sync

Same as above

0x00 to 0xFF
The packet sequence number starts from 0, incrementally in order.

Data 1, Data 2 ⋯Data n

Data format definition

Device-to-cloud

19

raw

len

Stage
(1 byte)

Message ID
(2 bytes)

Total packets
(1 byte)

0x01: Sync finished

Same as above

Total packets
For example, if a packet for the in-sync stage is delivered twice, the packets are two in total.

10.9 Combined unlocking records

Data transmission

dp_id
(1 byte)

dp_type
(1 byte)

dp_data_len
(2 bytes)

dp_data_value

Device-to-cloud

74

raw

len

Combined unlocking methods
(1 byte)

Unlocking method 1
(1 byte)

Hardware ID 1
(2 bytes)

Unlocking method 2
(1 byte)

Hardware ID 2
(2 bytes)

0x01: Fingerprint + Password
0x02: Fingerprint + Door card
0x03: Fingerprint + Face
0x04: Password + Door card
0x05: Password + Face
0x06: Door card + Face

```
<td align="left" nowrap>
    0x01: Password <br>0x02: Door card <br>0x03: Fingerprint <br>0x04:
       Face <br>0x05: Palm print <br>0x06: Finger vein <br>0xF0:
       Temporary password</th>
<td align="left" nowrap>0x0000 to 0xFFFE</td>
<td align="left" nowrap>Same as unlocking method 1</th>
<td align="left" nowrap>0x0000 to 0xFFFE</td>
```

11 Appendix: Validity period

Byte(s)

Meaning

Description

Example

1

Start time

Unsigned integer Data is four bytes long, stored in big-endian format.

Example: 123-456-789 (Unix timestamp) = 0x075BCD15 (hex) If the validity is permanent, the start time is 0x386CD300.

07

2

5B

3

CD

4

15

5

End time

Unsigned integer Data is four bytes long, stored in big-endian format.

Example: 999-999-999 (Unix timestamp) = 0x3B9AC9FF (hex) If the validity is permanent, the end time is 0x72BC9B7F.

3B

6

9A

7

C9

8

FF

9

The recurring patterns:

0x00: One-time

0x01: Daily schedule

0x02: Weekly schedule

0x03: Monthly schedule

10

Recurring flag 1

For a one-time schedule,
10 to 17 bytes are 0.

This field defaults
to 0x00.

This field defaults
to 0x00.

Bit 7: Default to 0
Bit 6: The 31st of a month
…
Bit 0: The 25th of a month

11

Recurring flag 2

This field defaults
to 0x00.

This field defaults
to 0x00.

Bit 7: The 24th of a month
…
Bit 0: The 17th of a month

12

Recurring flag 3

This field defaults
to 0x00.

This field defaults
to 0x00.

Bit 7: The 16th of a month
…
Bit 0: The 9th of a month

13

Recurring flag 4

This field defaults
to 0x00.

Bit 7: Default to 0
Bit 6: Saturday
…
Bit 1: Monday
Bit 0: Sunday

Bit 7: The 8th of a month
…
Bit 0: The 1st of a month

14

The start time 1 (hour) in a day

Start time: 08:30

08 (decimal)

15

The start time 2 (minute) in a day

30 (decimal)

16

The end time 1 (hour) in a day

End time: 20:30

20 (decimal)

17

The end time 2 (minute) in a day

30 (decimal)

When users add or modify unlocking methods, the recurring validity period and the access times are both applied. There are two use cases:

- When the access times are 0x00, this indicates permanent access. You only need to process the recurring pattern of the validity.
- When the recurring pattern is 0x00, this indicates one-time access. You only need to process the access times.

For example, schedule a password to be valid every Monday to Friday from 08:00 to 08:30 from 2018-01-26 08:00:00 to 2018-08-08 09:56:32. The validity is 0x 5A6A6F80 5B6A4DD0 02 0000003E 0800 081E.

- 2018-01-26 08:00:00 = 1516924800 (Unix timestamp) = 0x5A6A6F80 (hex)
- 2018-08-08 09:56:32 = 1533693392 (Unix timestamp) = 0x5B6A4DD0 (hex)
- The recurring pattern: 0x02 indicates weekly schedule.
- Recurring flag 1 = Recurring flag 2 = Recurring flag 3 = 0x00
- Recurring flag 4 = 0x3E (from Monday to Friday)
- The start time 1 is 0x08. The start time 2 is 0x00.
- The end time 1 is 0x08. The end time 2 is 0x1E.