Nuki Smart Lock API

V2.3.0

08.01.2025

Nuki Home Solutions GmbH Münzgrabenstrasse 92/4, 8010 Graz

1. Introduction

This document describes the bluetooth protocol used by the Nuki Smart Lock, the encryption functions in use and provides some communication examples.

2. Bluetooth GATT services

The Smartlock provides the following bluetooth GATT services.

Keyturner Initialization Service

Service-UUID: a92ee000-5501-11e4-916c-0800200c9a66

This service has no characteristics. It will only be used for advertising the uninitialized state of a Nuki Smart Lock.

Keyturner Pairing Service (Smart Lock 1 - 4th Generation)

Service-UUID: a92ee100-5501-11e4-916c-0800200c9a66

Keyturner Pairing Service (Smart Lock Ultra)

Service-UUID: a92ee300-5501-11e4-916c-0800200c9a66

General Data Input Output characteristic

The General Data Input Output characteristic is used to send data to or retrieve data from the Nuki Smart Lock. The central device can retrieve data manually by enabling indications in the client configuration. The client configuration will not be stored over subsequent connections.

Farther the central device can send data to the Nuki Smart Lock by using the GATT Write (Long) Characteristic Value sub-procedure.

All data sent to or read from this characteristic must be unencrypted.

Value

UUID: a92ee101-5501-11e4-916c-0800200c9a66

Type: uint8 array (max size is 20 Bytes)

Properties: write (long), indicate

Client configuration

Properties: write

Keyturner Service

Service-UUID: a92ee200-5501-11e4-916c-0800200c9a66

General Data Input Output characteristic

The General Data Input Output characteristic is used to retrieve data from the Nuki Smart Lock. The central device can retrieve data by enabling indications in the client configuration. The client configuration will not be stored over subsequent connections.

Farther the central device can send data to the Nuki Smart Lock by using the GATT Write (Long) Characteristic Value sub-procedure.

Value
UUID: a92ee201-5501-11e4-916c-0800200c9a66

Type: uint8 array (max size depending on MTU, fallback is limited to 20 Bytes)

Properties: write (long), indicate

Client configuration

Properties: write

Note: MTU exchange is supported since Smart Lock FW 1.9.3/2.7.20

User-Specific Data Input Output characteristic

The User-Specific Data Input Output characteristic is used to send data to or retrieve data from the Nuki Smart Lock. The central device can retrieve data by enabling indications in the client configuration. The client configuration will not be stored over subsequent connections.

Farther the central device can send data to the Nuki Smart Lock by using the GATT Write (Long) Characteristic Value sub-procedure.

All data sent to or read from this characteristic must be encrypted with the shared secret key of the connected user.

Value
UUID: a92ee202-5501-11e4-916c-0800200c9a66

Type: uint8 array (max size is 20 Bytes)

Properties: write (long), indicate

Client configuration

Properties: write

3. Message Format

Terminology

ADATA (additional data) data that is not encrypted (e.g. protocol data)

PDATA (plaintext) data to be encrypted and authenticated

ADATA:

- nonce (number only used once, NEVER reused with same secret key)
- authorization identifier
- message length

PDATA:

- command identifier
- payload data depending on command
- CRC

Transfer format for encrypted messages

ADATA			PDATA			
nonce	authorization identifier	message length	authorization identifier	command identifier	payload	CRC
24 Byte	4 Byte	2 Byte	4 Byte	2 Byte	n Byte	2 Byte

unencrypted	unencrypted	unencrypted	encrypted
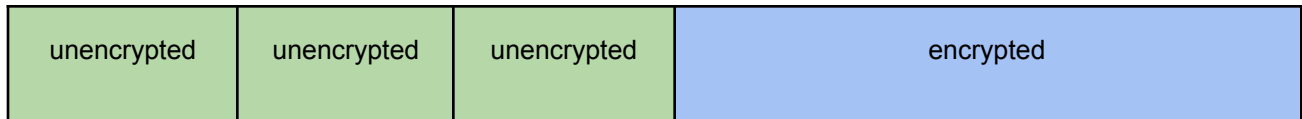
Transfer format for unencrypted messages

PDATA		
command identifier	payload	CRC
2 Byte	n Byte	2 Byte
unencrypted		
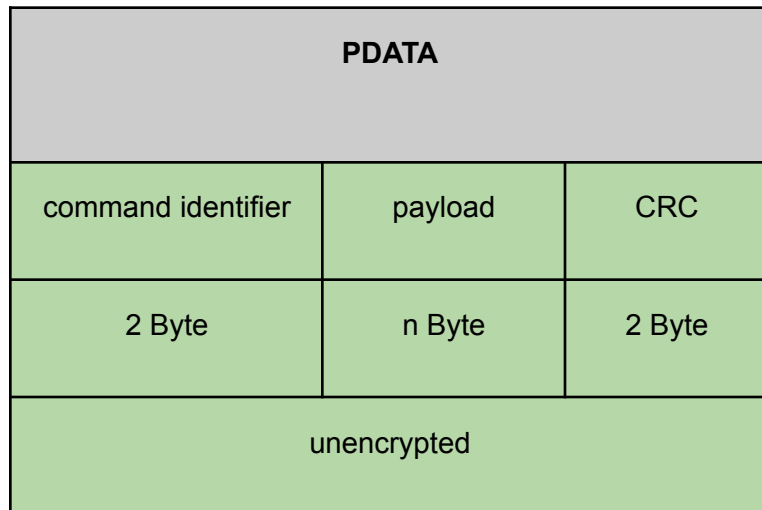
CRC calculation

Algorithm: CRC-CCITT

Polynomial representation: normal (0x1021)

Initial remainder: 0xFFFF

4. Encryption

The Nuki Smartlock uses the NaCl Cryptography Toolbox (http://nacl.cr.yp.to/) to encrypt the transferred data.

The following functions are needed to communicate with the Nuki Smartlock:

The Diffie-Hellman key function dh1

crypto_scalarmult_curve25519(s,sk,pk)

Necessary for the initial key exchange between the Nuki Smartlock and the client device.

The key derivation function kdf1

static const unsigned char _0[16];

static const unsigned char sigma[16] = "expand 32-byte k";

crypto_core_hsalsa20(k,_0,s,sigma)

Used to derive a long term secret key out of the shared key calculated by dh1

The authentication function h1

HMAC-SHA256

Used to calculate the authenticator during the authorization process between the Nuki Smartlock and the client device.

The encryption function e1

crypto_secretbox_xsalsa20poly1305 (c,m,mlen,n,k)

Used to encrypt any data once the authorization process has been completed

5. Commands

Command identifier	Command
0x0001	Request Data
0x0003	Public Key
0x0004	Challenge
0x0005	Authorization Authenticator

0x0006	Authorization Data
0x0007	Authorization-ID
0x0008	Remove Authorization Entry
0x0009	Request Authorization Entries
0x000A	Authorization Entry
0x000B	Authorization Data (Invite)
0x000C	Keyturner States
0x000D	Lock Action
0x000E	Status
0x000F	Most Recent Command
0x0010	Openings Closings Summary
0x0011	Battery Report
0x0012	Error Report
0x0013	Set Config

0x0014	Request Config
0x0015	Config
0x0019	Set Security PIN
0x001A	Request Calibration
0x001D	Request Reboot
0x001E	Authorization-ID Confirmation
0x001F	Authorization-ID (Invite)
0x0020	Verify Security PIN
0x0021	Update Time
0x0025	Update Authorization Entry
0x0027	Authorization Entry Count
0x0031	Request Log Entries
0x0032	Log Entry
0x0033	Log Entry Count

0x0034	Enable Logging
0x0035	Set Advanced Config
0x0036	Request Advanced Config
0x0037	Advanced Config
0x0039	Add Time Control Entry
0x003A	Time Control Entry ID
0x003B	Remove Time Control Entry
0x003C	Request Time Control Entries
0x003D	Time Control Entry Count
0x003E	Time Control Entry
0x003F	Update Time Control Entry
0x0041	Add Keypad Code
0x0042	Keypad Code ID
0x0043	Request Keypad Codes

0x0044	[Keypad Code Count](#)
0x0045	[Keypad Code](#)
0x0046	[Update Keypad Code](#)
0x0047	[Remove Keypad Code](#)
0x004C	[Authorization Info](#)
0x0100	[Simple Lock Action](#)

Authenticator	Calculated for all parts of a table (including the parts with dashed border)
solid border	This row is part of the transferred message.
dashed border	This row is not part of the transferred message, but included in the calculation of the authenticator.

Security PIN Handling

With the introduction of Smart Lock Ultra the Security PIN was increased from 4 digits to 6 digits. This affects the container which is used to represent the Security PIN in several commands, therefore this information has to be considered when such commands are being used for the communication with the Smart Lock.

Smart Lock (1 - 4th Generation)

Security-PIN	M	uint16	The 4-digit security pin

Smart Lock Ultra

Security-PIN	M	uint32	The 6-digit security pin

Request Data (0x0001)

Name	Requirement	Format	Additional Information
Command identifier	M	uint16	The identifier of the command to be executed by the Smart Lock.
Additional Data	M	uint8[n]	Depending on the command identifier additional data of length n will be added or not. The format of the additional data is described in the command specification.

Public Key (0x0003)

Name	Requirement	Format	Additional Information
Public Key	M	uint8[32]	The public key of the sender.

The Request Data command with the command identifier of the Public Key command initiates the authorization process of a new Nuki App or Nuki Bridge.

Challenge (0x0004)

Name	Requirement	Format	Additional Information
Nonce nK	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Authorization Authenticator (0x0005)

Name	Requirement	Format	Additional Information
Authenticator	M	uint8[32]	The authenticator of the sender for the current message.
Public-Key A/B/F	M	uint8[32]	The public key of the Nuki App, Nuki Bridge or Nuki Fob to be authorized.

Public Key K	M	uint8[32]	The public key of the Smart Lock..
Nonce nK	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Authorization Data (0x0006)

Smart Lock (1 - 4th Generation)

Name	Require ment	Format	Additional Information
Authenticator	M	uint8[32]	The authenticator of the sender for the current message.
ID Type	M	uint8	The type of the ID to be authorized. 0 … App 1 … Bridge 2 … Fob 3 … Keypad
App-ID/Bridge-ID/ Fob-ID	M	uint32	The ID of the Nuki App, Nuki Bridge or Nuki Fob to be authorized.
Name	M	uint8[32]	The name to be displayed for this authorization.
Nonce n A/B/F	M	uint8[32]	An arbitrary number used only

			once to resist replay attacks. (unpredictable, probabilistic non-reuse)
Nonce n K	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Smart Lock Ultra

Name	Require ment	Format	Additional Information
App-ID	M	uint32	The ID of the Nuki App
Name	M	uint8[32]	The name to be displayed for this authorization
Security-PIN	M	uint32	The security pin

Authorization-ID (0x0007)

Smart Lock (1 - 4th Generation)

Name	Require ment	Format	Additional Information
Authenticator	M	uint8[32]	The authenticator of the sender for the current message.

Authorization-ID	M	uint32	The unique identifier of the recently authorized Nuki App or Nuk Bridge.
UUID	M	uint8[16]	Random identifier unique per Smart Lock and not altered until the Smart Lock is reset to factory defaults.
Nonce n K	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)
Nonce n A/B/F	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Smart Lock Ultra

Name	Require ment	Format	Additional Information
Authorization-ID	M	uint32	The unique identifier of the recently authorized Nuki App or Nuk Bridge.
UUID	M	uint8[16]	Random identifier unique per Smart Lock and not altered until the Smart Lock is reset to factory defaults.

Authorization-ID Confirmation (0x001E)

Name	Require ment	Format	Additional Information
Authenticator	M	uint8[32]	The authenticator of the sender for the current message.
Authorization-ID	M	uint32	The unique identifier of the recently authorized Nuki App or Nuki Bridge.
Nonce n K	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Remove Authorization Entry (0x0008)

Name	Require ment	Format	Additional Information
Authorization-ID	M	uint32	The Authorization-ID to be removed.
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Request Authorization Entries (0x0009)

Name	Requirement	Format	Additional Information
Offset	M	uint16	The start offset to be read.
Count	M	uint16	The number of authorizations to be read, starting at the specified offset.
Filter for Auth ID type	O	uint8	Filter to receive only dedicated Auth ID type as response Allowed values: 0x00 … App 0x01 … Bridge 0x02 … Fob 0x03 … Keypad 0x04 … Door sensor 0x05 … Keypad 2 Only supported by Smart Lock 4th Generation and Ultra.
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Authorization Entry (0x000A)

Name	Requirement	Format	Additional Information
Authorization-ID	M	uint32	The Authorization-ID.
ID Type	M	uint8	The type of the ID. 0 … App 1 … Bridge 2 … Fob 3 … Keypad
Name	M	uint8[32]	The Name of the Nuki App or Nuki Bridge.
Enabled	M	unit8	Flag indicating if this authorization is enabled.
Remote allowed	M	uint8	Flag indicating if requests proxied by the nuki bridge shall be allowed.
Date created	M	uint8[7]	The creation date. *Format:* | Year	uint16 | | Month | uint8 | | Day | uint8 | | Hour | uint8 | | Minute | uint8 |

Format table detail for Date created:

Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8

				Second	uint8	
Date last active	M	uint8[7]	The date of the last received request from this authorization. *Format:* 	Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Lock count	M	uint16	The lock counter.
Time limited	M	uint8	Flag indicating if this authorization is restricted to access only at certain times. The following fields are appended only if this flag is set.
Allowed from date	M	uint8[7]	The start timestamp from which access should be allowed. *Format:* 	Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	

Allowed until date	M	uint8[7]	The end timestamp until access should be allowed. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Allowed weekdays	M	uint8	Bitmask for allowed weekdays: `0 0 0 0 0 0 0 0` -- MO TU WE TH FR SA SU If no bit is set, all weekdays are allowed.
Allowed from time	M	uint8[2]	The start time per day from which access should be allowed. *Format:* | Hour	uint8
Minute	uint8	
Allowed until time	M	uint8[2]	The end time per day until access should be allowed. *Format:* | Hour	uint8
Minute	uint8	

The Nuki Smart Lock will continue sending Authorization Entry commands until the requested count is reached or no more authorization entries are available.

The first returned authorization entry represents the own authorization.

Authorization Data (Invite) (0x000B)

Name	Require ment	Format	Additional Information
Name	M	uint8[32]	The name to be displayed for this authorization.
ID Type	M	uint8	The type of the ID to be authorized. 0 … App 1 … Bridge 2 … Fob 3 … Keypad
Shared Key	M	uint8[32]	The generated shared key for this authorization.
Remote allowed	M	uint8	Flag indicating if requests proxied by the nuki bridge shall be allowed.
Time limited	M	unit8	Flag indicating if this authorization is restricted to access only at certain times.
Allowed from date	M	uint8[7]	The start timestamp from which access should be allowed.

<table>
<tr><td colspan="4">

Format:

Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8

</td></tr>
</table>

			Format: | Year	uint16 | |---|---|
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Allowed until date	M	uint8[7]	The end timestamp until access should be allowed. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	

Allowed weekdays	M	uint8	Bitmask for allowed weekdays:
			`0 0 0 0 0 0 0 0`
			
			`-- MO TU WE TH FR SA SU`
			
			If no bit is set, all weekdays are allowed.

Allowed from time	M	uint8[2]	The start time per day from which access should be allowed. *Format:*

				Hour	uint8
				Minute	uint8
Allowed until time	M	uint8[2]	The end time per day until access should be allowed. *Format:* 	Hour	uint8	 	Minute	uint8	
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	MM	uint16 uint32	The security pin, as defined in [Security PIN handling](#).

Authorization-ID (Invite) (0x001F)

Name	Require ment	Format	Additional Information
Authorization-ID	M	uint32	The unique identifier of the recently authorized Nuki App or Nuki Bridge.
Date created	M	uint8[7]	The creation date. *Format:* 	Year	uint16	

			Month	uint8	
			Day	uint8	
			Hour	uint8	
			Minute	uint8	
			Second	uint8	

Update Authorization Entry (0x0025)

Name	Require ment	Format	Additional Information
Authorization-ID	M	uint32	The authorization id.
Name	M	uint8[32]	The name to be displayed for this authorization.
Enabled	M	unit8	Flag indicating if this authorization is enabled.
Remote allowed	M	uint8	Flag indicating if requests proxied by the nuki bridge shall be allowed.
Time limited	M	unit8	Flag indicating if this authorization is restricted to access only at certain times.

Allowed from date	M	uint8[7]	The start timestamp from which access should be allowed
			
			Format:
			    Year uint16
			    Month uint8
			    Day uint8
			    Hour uint8
			    Minute uint8
			    Second uint8

Allowed until date	M	uint8[7]	The end timestamp until access should be allowed
			
			Format:
			    Year uint16
			    Month uint8

			Day uint8 Hour uint8 Minute uint8 Second uint8

Allowed weekdays	M	uint8	Bitmask for allowed weekdays:
			  0 0 0 0 0 0 0 0
			  -- MO TU WE TH FR SA SU
			
			If no bit is set, all weekdays are allowed.

Allowed from time	M	uint8[2]	The start time per day from which access should be allowed.
			
			Format:
			    Hour uint8
			    Minute uint8

Allowed until time	M	uint8[2]	The end time per day until access should be allowed.
			
			Format:
			    Hour uint8
			    Minute uint8

Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Keyturner States (0x000C)

Name	Requirement	Format	Additional Information
Nuki State	M	uint8	The current operation state of the Smart Lock 0x00 Uninitialized 0x01 Pairing Mode 0x02 Door Mode 0x04 Maintenance Mode
Lock State	M	uint8	The current state of the locking mechanism within the Smart Lock

			0x00 uncalibrated 0x01 locked 0x02 unlocking 0x03 unlocked 0x04 locking 0x05 unlatched 0x06 unlocked (lock 'n' go active) 0x07 unlatching 0xFC calibration 0xFD boot run 0xFE motor blocked 0xFF undefined

Trigger	M	uint8	The trigger, that caused the state change of the unlock mechanism within the Smart Lock
			
			0x00 system
			   ● via bluetooth command
			
			0x01 manual
			   ● by using a key from outside the door
			   ● by rotating the wheel on the inside
			
			0x02 button
			   ● by pressing the Smart Locks button
			
			0x03 automatic
			   ● Executed automatically (e.g. at a specific time) by the Smart Lock
			
			0x06 auto lock
			   ● Auto relock of the Smart Lock

Current Time	M	uint8[7]	Current timestamp *Format:* Year uint16 Month uint8 Day uint8 Hour uint8 Minute uint8 Second uint8
Timezone offset	M	sint16	The timezone offset (UTC) in minutes

Critical Battery state	M	uint8	This flag signals a critical battery state.
			
			Format
			    Bit 0 Smart Lock Battery State Critical
			    Bit 1 Charging Flag
			    Bit 2-7 Smart Lock Battery in %
			
			Note:
			Bits 2-7 represent the battery load state from 0-100% in steps of two (e.g. 50% is represented as 25).

Config update count	M	uint8	Current count of modifications to the internal config
Lock 'n' Go timer	M	uint8	Current status of the lock 'n' go timer or 0 if no lock 'n' go is active
Last Lock Action	M	uint8	The most recent Lock Action that has been performed
Last Lock Action trigger	M	uint8	The trigger that caused the most recent lock action
Last Lock Action completion status	M	uint8	The completion status of the most recent lock action
Door sensor state	M	uint8	The current door sensor state Smart Lock (1.0 - 2.0) 0x00 … Unavailable 0x01 … Deactivated 0x02 … Door Closed 0x03 … Door Opened 0x04 … Door State Unknown 0x05 … Calibrating Smart Lock (3.0 - Ultra) 0x00 … Unavailable (=not paired) 0x02 … Door Closed 0x03 … Door Opened 0x10 … Uncalibrated 0xF0 … Tampered 0xFF … Unknown
Nightmode active	M	uint8	Flag indicating whether or not nightmode is currently active

Accessory Battery State	M	uint8	Bitmask, which represents the current battery state of connected accessories. For now only the Keypad is being supported. *Format*: Bit 0 Feature supported by Keypad Bit 1 Keypad Battery State Critical Bit 2 Feature supported by Door Sensor Bit 3 Door Sensor Battery State Critical Bit 4-7 <reserved>
Remote Access Status	M	uint8	*Format:* Bit 0 … SSE uplink available via BR/WiFi/Thread Bit 1 ... Bridge paired Bit 2 … SSE connection via WiFi Bit 3 ... SSE connection established Bit 4 ... SSE connection via Thread Bit 5 … Thread SSE uplink enabled (manual setting from user) Bit 6 … NAT64 available via Thread (potential SSE uplink) Only supported by Smart Lock 4th Generation and Ultra.
Remote Access - BLE connection strength	M	int8	RSSI of BLE connection between the Nuki Bridge and the Nuki Smart Lock everything below 0 represents the latest RSSI 0x00 … invalid 0x01 … not supported Only supported by Smart Lock 4th Generation and Ultra.
Remote Access - WiFi Connection strength	M	int8	RSSI of WiFi connection between the Nuki Smart Lock and the WiFi router everything below 0 represents the latest RSSI 0x00 … invalid 0x01 … not supported

			Only supported by Smart Lock 4th Generation and Ultra.

WiFi Connection status	M	uint8	Container representing the health status of the WiFi and SSE server connection.
			
			Format - connection established:
			Bit 0-1 … 0x00 WiFi disabled (manual setting from the user)
			    0x01 WiFi disconnected
			    0x02 WiFi connecting
			    0x03 WiFi connected
			Bit 2-3 … 0x00 SSE suspended
			    0x01 SSE not reachable
			    0x02 SSE connecting
			    0x03 SSE connected
			Bit 4-7 … WiFi quality
			
			Only supported by Smart Lock 4th Generation and Ultra.

MQTT API Connection Status	M	uint8	Container representing the connection status of the MQTT API. Bit 0-1 0x00 … MQTT API disabled (manual setting from user) 0x01 … MQTT API disconnected 0x02 … MQTT API connecting 0x03 … MQTT API connected Bit 2 0x00 ... MQTT API done via WiFi (default value) 0x01 ... MQTT API done via Thread Only supported by Smart Lock 4th Generation and Ultra.
Thread Connection Status	M	uint8	Container representing the connection status of the Thread interface Bit 0-1 0x00 Matter disabled (manual setting from the user) 0x01 Thread disconnected 0x02 Thread connecting 0x03 Thread connected

			Bit 2-3 0x00 SSE suspended 0x01 SSE not reachable 0x02 SSE connecting 0x03 SSE connected Bit 4-7 Bit 4 Matter commissioning mode active Bit 5 WiFi suspended because of Thread SSE uplink Bit 6 <reserved> Bit 7 <reserved> Only supported by Smart Lock 4th Generation and Ultra.

Lock Action (0x000D)

Name	Require ment	Format	Additional Information
Lock Action	M	uint8	The action to be executed. **0x01 unlock** **0x02 lock** **0x03 unlatch** **0x04 lock 'n' go** **0x05 lock 'n' go with unlatch** **0x06 full lock** **0x81 fob action 1** **0x82 fob action 2** **0x83 fob action 3**
App-ID/Bridge-ID/Fob -ID	M	uint32	The ID of the Nuki App, Nuki Bridge or Nuki Fob sending the command.

Flags	M	uint8	Bitmask containing some flags: Bitmask for allowed weekdays: 0 0 0 0 0 0 0 0 -- -- -- -- -- -- FO AU AU Auto Unlock FO Force Other bits are reserved for future use.
Name suffix	O	uint8[20]	Optional parameter containing a suffix which should be appended to the log entry.
Nonce n K	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Status (0x000E)

Name	Requirement	Format	Additional Information
Status	M	uint8	The status of the most recently executed action.

Most Recent Command (0x000F)

Name	Requirement	Format	Additional Information

Name	Require ment	Format	Additional Information
Command identifier	M	uint16	The identifier of the most recently executed command by the Smart Lock.

Openings Closings Summary (0x0010)

Name	Require ment	Format	Additional Information
Openings total	M	uint16	The number of openings in total
Closings total	M	uint16	The number of closings in total.
Openings since boot	M	uint16	The number of openings since the Smart Lock booted
Closings since boot	M	uint16	The number of closings since the Smart Lock booted

Battery Report (0x0011)

Name	Requirem ent	Format	Additional Information
Battery Drain	M	uint16	The drain of the last lock action in Milliwattseconds (mWs).

Battery Voltage	M	uint16	The current battery voltage in Millivolts (mV).
Critical Battery state	M	uint8	This flag signals a critical battery state. 0x00 ok 0x01 critical
Lock Action	M	uint8	The type of the last executed lock action or 0x00 if no lock action has been executedSee (Lock Action)
Start Voltage	M	uint16	The voltage (mV) at the beginning of the last lock action
Lowest Voltage	M	uint16	The lowest voltage (mV) reached during the last lock action
Lock Distance	M	uint16	The total distance (in degrees) during the last lock action
Start Temperature	M	sint8	The die temperature at the beginning of the last lock action
Max Turn Current	M	uint16	The highest current of the turn motor during the last lock action
Battery Resistance	M	uint16	The resistance of the batteries

Error Report (0x0012)

Name	Requirement	Format	Additional Information
Error Code	M	sint8	The error code.
Command identifier	M	uint16	The identifier of the command.

Set Config (0x0013)

Name	Requirement	Format	Additional Information
Name	M	uint8[32]	The name of the Smart Lock..
Latitude	M	float	The latitude of the Smart Locks geoposition.
Longitude	M	float	The longitude of the Smart Locks geoposition.
Auto unlatch	M	uint8	This flag indicates whether or not the door shall be unlatched by manually operating a door handle from the outside.
Pairing enabled	M	uint8	This flag indicates whether or not activating the pairing mode via button should be enabled.

Button enabled	M	uint8	This flag indicates whether or not the button should be enabled.
LED flash enabled	M	uint8	This flag indicates whether or not the flashing LED should be enabled to signal an unlocked door.
LED brightness	M	uint8	The LED brightness level. Possible values are 0 to 5 0 = off, …, 5 = max
Timezone offset	M	sint16	The timezone offset (UTC) in minutes
DST mode	M	uint8	The desired daylight saving time mode. 0x00 disabled 0x01 european
Fob action 1	M	uint8	The desired action, if a Nuki Fob is pressed once. 0x00 no action 0x01 unlock 0x02 lock 0x03 lock 'n' go 0x04 intelligent (unlock if locked, lock if unlocked) If the auto unlatch flag has been set, the Smart Lock shall perform the unlatch operation in any "unlock" case. (0x01, 0x03 and 0x04)

Fob action 2	M	uint8	The desired action, if a Nuki Fob is pressed twice. See "Fob action 1" for possible values.
Fob action 3	M	uint8	The desired action, if a Nuki Fob is pressed three times. See "Fob action 1" for possible values.
Single Lock	M	uint8	Flag indicating, if only a single lock should be performed
Advertising Mode	M	uint8	The desired advertising mode. 0x00 Automatic 0x01 Normal 0x02 Slow 0x03 Slowest
Timezone ID	M	uint16	The id of the current timezone or 0xFFFF if timezones are not supported See List of timezone IDs
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Request Config (0x0014)

Name	Require ment	Format	Additional Information
Nonce n K	M	uint8[32]	The nonce received from the challenge.

Config (0x0015)

Name	Require ment	Format	Additional Information
Nuki-ID	M	uint32	The unique identifier of the Smart Lock.
Name	M	uint8[32]	The name of the Smart Lock.
Latitude	M	float	The latitude of the Smart Locks geoposition.
Longitude	M	float	The longitude of the Smart Locks geoposition.
Auto unlatch	M	uint8	This flag indicates whether or not the door shall be unlatched by manually operating a door handle from the outside.
Pairing enabled	M	uint8	This flag indicates whether or not the pairing mode should be

			enabled.
Button enabled	M	uint8	This flag indicates whether or not the button should be enabled.
LED enabled	M	uint8	This flag indicates whether or not the LED should be enabled to signal an unlocked door.
LED brightness	M	uint8	The LED brightness level. Possible values are 0 to 5 0 = off, …, 5 = max
Current Time	M	uint8[7]	Current timestamp *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Timezone offset	M	sint16	The timezone offset (UTC) in minutes
DST mode	M	uint8	The desired daylight saving time mode. 0x00 disabled 0x01 european

Has fob	M	uint8	This flag indicates whether or not a Nuki Fob has been paired to this Nuki.
Fob action 1	M	uint8	The desired action, if a Nuki Fob is pressed once. 0x00 no action 0x01 unlock 0x02 lock 0x03 lock 'n' go 0x04 intelligent (unlock if locked, lock if unlocked)
Fob action 2	M	uint8	The desired action, if a Nuki Fob is pressed twice. See "Fob action 1" for possible values.
Fob action 3	M	uint8	The desired action, if a Nuki Fob is pressed three times. See "Fob action 1" for possible values.
Single Lock	M	uint8	Flag indicating, if only a single lock should be performed
Advertising Mode	M	uint8	The desired advertising mode. 0x00 … Automatic 0x01 … Normal 0x02 … Slow 0x03 … Slowest

Has keypad	M	uint8	This flag indicates whether or not a Nuki Keypad has been paired to this Nuki.
Firmware version	M	uint8[3]	The currently installed firmware version of the Smart Lock
Hardware revision	M	uint8[2]	The hardware revision number
HomeKit status	M	uint8	Smart Lock 0x00 … not available Smart Lock (2.0 - 3.0) 0x01 … disabled 0x02 … enabled 0x03 … enabled & paired Smart Lock (4th Generation - Ultra) 0x00 … deprecated
Timezone ID	M	uint16	The id of the current timezone or 0xFFFF if timezones are not supported See List of timezone IDs
Device Type	M	uint8	Unique type id, which represents a product family 0x04 ... Smart Lock 3.0 / 4th gen 0x05 … Smart Lock Ultra Only supported by Smart Lock 3.0, 4th Generation and Ultra.
Capabilities	M	uint8	Hardware capabilities of the Smart Lock

			Format: bit 0 … WiFi enabled bit 1 ... Thread/Matter enabled bit 2-7 … reserved Only supported by Smart Lock 3.0, 4th Generation and Ultra.
Has keypad2	M	uint8	This flag indicates whether or not a Nuki Keypad 2.0 has been paired to this Nuki actor. 0x00 … KP2 not paired 0x01 … KP2 paired Only supported by Smart Lock 3.0, 4th Generation and Ultra.
Matter status	M	uint8	The status of the Matter plugin 0x00 … not available 0x01 ... disabled 0x02 … disabled (all necessary information is on the SL4G) 0x03 … enabled 0x04 … enabled & paired Only supported by Smart Lock 4th Generation and Ultra.

Set Security PIN (0x0019)

Name	Requirement	Format	Additional Information
PIN	M	uint16 uint32	The new security pin, as defined in Security PIN handling.

Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Verify Security PIN (0x0020)

Name	Require ment	Format	Additional Information
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Request Calibration (0x001A)

Name	Require ment	Format	Additional Information
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Request Reboot (0x001D)

Name	Requirement	Format	Additional Information
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling]().

Update Time (0x0021)

Name	Requirement	Format	Additional Information
Time	M	uint8[7]	Timestamp *Format:* <table><tr><td>Year</td><td>uint16</td></tr><tr><td>Month</td><td>uint8</td></tr><tr><td>Day</td><td>uint8</td></tr><tr><td>Hour</td><td>uint8</td></tr><tr><td>Minute</td><td>uint8</td></tr><tr><td>Second</td><td>uint8</td></tr></table>
Nonce n K	M	uint8[32]	The nonce received from the challenge.

| Security-PIN | M | uint16

uint32 | The security pin, as defined in [Security PIN handling](#). |
|---|---|---|---|

Authorization Entry Count (0x0027)

Name	Requirement	Format	Additional Information
Count	M	uint16	The total number of authorization entries

Request Log Entries (0x0031)

Name	Requirement	Format	Additional Information
Start index	M	uint32	The index where to start reading log entries.Log entries older or newer (based on sort order) than the provided index will be returned, not the entry for the provided index itself.

If 0 the oldest or most recent [Count] entries are returned, based on [Sort order]. |
| Count | M | uint16 | The number of log entries to be read, starting at the specified start index. |
| Sort order | M | uint8 | The desired sort order. |

			0x00 ascending 0x01 descending
Total count	M	uint8	Flag indicating whether or not a Log Entry Count should be returned, prior sending the requested Log Entries
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Log Entry (0x0032)

Name	Require ment	Format	Additional Information
Index	M	uint32	The index of the log entry.
Timestamp	M	uint8[7]	The timestamp. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	

Auth-ID	M	uint32	The authorization id.
Name	M	uint8[32]	The name of the authorization.
Type	M	uint8	0x01 Logging enabled/disabled 0x02 Lock action 0x03 Calibration 0x04 Initialization run 0x05 Keypad action 0x06 Door sensor 0x07 Door sensor logging enabled/disabled
Data	M	uint8[x]	*Type 0x01:* x = 1 0x00 Logging disabled 0x01 Logging enabled *Type 0x02, 0x03 and 0x04:* x = 4 byte 1: Lock Action byte 2: Trigger byte 3: Flags byte 4: Completion status 0x00 … Success 0x01 … Motor blocked 0x02 … Canceled 0x03 … Too recent 0x04 … Busy 0x05 … Low motor voltage

			voltage
			0x06 … Clutch failure
			0x07 … Motor power failure
			0x08 … Incomplete
			0x09 … Rejected
			0x0A … Rejected (Nightmode)
			0x0B … Handle not lifted
			0xFE … Other error
			0xFF … UNKNOWN
			Type 0x05:
			x = 5
			byte 1: Lock Action
			byte 2: Source
			byte 3: Completion status
			Same as Type 0x04
			additionally:
			0xE0 … Invalid Code
			0xE1 … Invalid Fingerprint
			bytes 4-5: Code ID (uint16)
			Type 0x06:
			x = 1
			0x00 Door opened
			0x01 Door closed
			0x02 Sensor jammed
			0x03 Sensor tampered
			Type 0x07:

			x = 1
			0x00 Door Sensor Logging disabled
			0x01 Door Sensor Logging enabled

The Nuki Smart Lock will continue sending Log Entry commands until the requested count is reached or no more log entries are available.

Log Entry Count (0x0033)

Name	Requirement	Format	Additional Information
Logging enabled	M	uint8	This flag indicates whether or not logging is enabled.
Count	M	uint16	Total number of log entries which are available with the given start index and sort order
Door Sensor Enabled	M	uint8	Flag indicating if door sensor should be enabled
Door Sensor Logging Enabled	M	uint8	Flag indicating if door sensor logging should be enabled

Enable Logging (0x0034)

Name	Requirement	Format	Additional Information

Enabled	M	uint8	Flag indicating if logging should be enabled.
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling]().

Set Advanced Config (0x0035)

Name	Requirement	Format	Additional Information
Unlocked Position Offset Degrees	M	sint16	Offset that alters the unlocked position.
Locked Position Offset Degrees	M	sint16	Offset that alters the locked position.
Single Locked Position Offset Degrees	M	sint16	Offset that alters the single locked position.
Unlocked To Locked Transition Offset Degrees	M	sint16	Offset that alters the position where transition from unlocked to locked happens.
Lock 'n' Go timeout	M	uint8	Timeout for lock 'n' go
Single button press action	M	uint8	The desired action, if the button is pressed once. 0x00 no action 0x01 intelligent (unlock if locked, lock if unlocked) 0x02 unlock 0x03 lock 0x04 unlatch 0x05 lock 'n' go (without unlatch) 0x06 show status

Double button press action	M	uint8	The desired action, if the button is pressed twice. 0x00 no action 0x01 intelligent (unlock if locked, lock if unlocked) 0x02 unlock 0x03 lock 0x04 unlatch 0x05 lock 'n' go (without unlatch) 0x06 show status
Detached cylinder	M	uint8	Flag that indicates that the inner side of the used cylinder is detached from the outer side and therefore the Smart Lock won't recognize if someone operates the door by using a key
Battery type	M	uint8	The type of the batteries present in the smart lock. 0x00 Alkali 0x01 Accumulators 0x02 Lithium Batteries
Automatic battery type detection	M	uint8	Flag that indicates if the automatic detection of the battery type is enabled
Unlatch duration	M	uint8	Duration in seconds for holding the latch in unlatched position.
Auto lock timeout	M	uint16	Seconds until the smart lock relocks itself after it has been unlocked. *Minimum value: 2*
Auto unlock disabled	M	uint8	Flag that indicates if auto unlock should be disabled in general
Nightmode enabled	M	uint8	Flag that indicates if nightmode is enabled

Nightmode start time	M	uint8[2]	*Format:*
			    Hour uint8
			    Minute uint8

Nightmode end time	M	uint8[2]	*Format:*
			    Hour uint8
			    Minute uint8

Nightmode auto lock enabled	M	uint8	Flag that indicates if auto lock should be enabled during nightmode
Nightmode auto unlock disabled	M	uint8	Flag that indicates if auto unlock should be disabled during nightmode
Nightmode immediate lock on start	M	uint8	Flag that indicates if door should be immediately locked on nightmode start
Auto lock enabled	M	uint8	Flag that indicates if auto lock is enabled
Immediate auto lock enabled	M	uint8	Flag that indicates if auto lock should be performed immediately after the door has been closed (requires active door sensor) *Also 0x00 if not supported*
Auto update enabled	M	uint8	Flag that indicated if automatic firmware updates should be enabled
Motor speed	M	uint8	Field used for setting the motor speed. Allowed values: 0x00 … Standard (default value) 0x01 … Insane 0x02 … Gentle Only supported by Smart Lock Ultra.
Enable slow speed during NightMode	M	uint8	Flag indicating if the slow speed shall be applied during Night Mode. Allowed values: 0x00 … false 0x01 … true Only supported by Smart Lock Ultra.
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling](#).

Request Advanced Config (0x0036)

Name	Requirement	Format	Additional Information
Nonce n_K	M	uint8[32]	The nonce received from the challenge.

Advanced Config (0x0037)

Name	Requirement	Format	Additional Information
Total Degrees	M	uint16	The absolute total position in degrees that has been reached during calibration.
Unlocked Position Offset Degrees	M	sint16	Offset that alters the unlocked position.
Locked Position Offset Degrees	M	sint16	Offset that alters the locked position.
Single Locked Position Offset Degrees	M	sint16	Offset that alters the single locked position.
Unlocked To Locked Transition Offset Degrees	M	sint16	Offset that alters the position where transition from unlocked to locked happens.
Lock 'n' Go timeout	M	uint8	Duration of the unlocked status during lock 'n' go
Single button press action	M	uint8	The desired action, if the button is pressed once. ***Defaults to 0x01.*** 0x00 no action **0x01 intelligent (unlock if locked, lock if unlocked)** 0x02 unlock 0x03 lock 0x04 unlatch 0x05 lock 'n' go (without unlatch) 0x06 show status

Double button press action	M	uint8	The desired action, if the button is pressed twice. ***Defaults to 0x05.*** 0x00 no action 0x01 intelligent (unlock if locked, lock if unlocked) 0x02 unlock 0x03 lock 0x04 unlatch **0x05 lock 'n' go (without unlatch)** 0x06 show status
Detached cylinder	M	uint8	Flag that indicates that the inner side of the used cylinder is detached from the outer side and therefore the Smart Lock won't recognize if someone operates the door by using a key
Battery type	M	uint8	The type of the batteries present in the smart lock. ***Defaults to 0x00*** **0x00 Alkali** 0x01 Akkumulators 0x02 Lithium Batteries
Automatic battery type detection	M	uint8	Flag that indicates if the automatic detection of the battery type is enabled
Unlatch duration	M	uint8	Duration in seconds for holding the latch in unlatched position.
Auto lock timeout	M	uint16	Seconds until the smart lock relocks itself after it has been unlocked.
Auto unlock disabled	M	uint8	Flag that indicates if auto unlock should be disabled in general
Nightmode enabled	M	uint8	Flag that indicates if nightmode is enabled
Nightmode start time	M	uint8[2]	*Format:* Hour uint8 Minute uint8
Nightmode end time	M	uint8[2]	*Format:* Hour uint8 Minute uint8

Nightmode auto lock enabled	M	uint8	Flag that indicates if auto lock should be enabled during nightmode
Nightmode auto unlock disabled	M	uint8	Flag that indicates if auto unlock should be disabled during nightmode
Nightmode immediate lock on start	M	uint8	Flag that indicates if door should be immediately locked on nightmode start
Auto lock enabled	M	uint8	Flag that indicates if auto lock is enabled
Immediate auto lock enabled	M	uint8	Flag that indicates if auto lock should be performed immediately after the door has been closed (requires active door sensor) 0x00 … disabled 0x01 … enabled 0xFF … not supported (e.g. Smart Lock 1.0)
Auto update enabled	M	uint8	Flag that indicates if automatic firmware updates should be enabled
Motor speed	M	uint8	Field used for setting the motor speed. Allowed values: 0x00 … Standard (default value) 0x01 … Insane 0x02 … Gentle Only supported by Smart Lock Ultra.
Enable slow speed during NightMode	M	uint8	Flag indicating if the slow speed shall be applied during Night Mode. Allowed values: 0x00 … false 0x01 … true Only supported by Smart Lock Ultra.

Add Time Control Entry (0x0039)

Name	Require ment	Format	Additional Information
Weekdays	M	uint8	Bitmask for allowed weekdays: 0 0 0 0 0 0 0 0 -- MO TU WE TH FR SA SU If no bit is set, all weekdays are allowed.
Time	M	uint8[2]	*Format:* | Hour	uint8
Minute	uint8	
Lock action	M	uint8	The desired lock actionSee Lock Action
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Time Control Entry ID (0x003A)

Name	Require ment	Format	Additional Information

Entry ID	M	uint8	The unique identifier of the recently created time control entry.

Remove Time Control Entry (0x003B)

Name	Require ment	Format	Additional Information
Entry ID	M	uint8	The id of the entry to be removed.
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling]().

Request Time Control Entries (0x003C)

Name	Require ment	Format	Additional Information
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling]().

Time Control Entry Count (0x003D)

Name	Require ment	Format	Additional Information
Count	M	uint8	The total number of time control entries

Time Control Entry (0x003E)

Name	Require ment	Format	Additional Information
Entry ID	M	uint8	The id of the entry.
Enabled	M	unit8	Flag indicating if this authorization is enabled.
Weekdays	M	unit8	Bitmask for allowed weekdays: 0 0 0 0 0 0 0 0 -- MO TU WE TH FR SA SU If no bit is set, all weekdays are allowed.
Time	M	uint8[2]	*Format:* | Hour	uint8 | | Minute | uint8 |

Lock action	M	uint8	The desired lock action See Lock Action

Update Time Control Entry (0x003F)

Name	Requirement	Format	Additional Information
Entry ID	M	uint8	The id of the entry.
Enabled	M	unit8	Flag indicating if this authorization is enabled.
Weekdays	M	uint8	Bitmask for allowed weekdays: 0 0 0 0 0 0 0 -- MO TU WE TH FR SA SU If no bit is set, all weekdays are allowed.
Time	M	uint8[2]	*Format:* <table><tr><td>Hour</td><td>uint8</td></tr><tr><td>Minute</td><td>uint8</td></tr></table>
Lock action	M	uint8	The desired lock actionSee Lock Action
Nonce n K	M	uint8[32]	The nonce received from the challenge.

Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling](#).

Add Keypad Code (0x0041)

Name	Require ment	Format	Additional Information
Code	M	uint32	The code for this entry.
Name	M	uint8[20]	The name to be displayed for this entry.
Time limited	M	unit8	Flag indicating if this entry is restricted to access only at certain times.
Allowed from date	M	uint8[7]	The start timestamp from which access should be allowed. *Format:* <table><tr><td>Year</td><td>uint16</td></tr><tr><td>Month</td><td>uint8</td></tr><tr><td>Day</td><td>uint8</td></tr><tr><td>Hour</td><td>uint8</td></tr><tr><td>Minute</td><td>uint8</td></tr><tr><td>Second</td><td>uint8</td></tr></table>
Allowed until date	M	uint8[7]	The end timestamp until access should be allowed.

			Format: <table><tr><td>Year</td><td>uint16</td></tr><tr><td>Month</td><td>uint8</td></tr><tr><td>Day</td><td>uint8</td></tr><tr><td>Hour</td><td>uint8</td></tr><tr><td>Minute</td><td>uint8</td></tr><tr><td>Second</td><td>uint8</td></tr></table>

Allowed weekdays	M	uint8	Bitmask for allowed weekdays:
			`0 0 0 0 0 0 0 0`
			`-- MO TU WE TH FR SA SU`
			
			If no bit is set, all weekdays are allowed.

Allowed from time	M	uint8[2]	The start time per day from which access should be allowed. *Format:* <table><tr><td>Hour</td><td>uint8</td></tr><tr><td>Minute</td><td>uint8</td></tr></table>
Allowed until time	M	uint8[2]	The end time per day until access should be allowed. *Format:* <table><tr><td>Hour</td><td>uint8</td></tr><tr><td>Minute</td><td>uint8</td></tr></table>

Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling](#).

Keypad Code ID (0x0042)

Name	Require ment	Format	Additional Information
Code ID	M	uint16	The unique identifier of the recently created Keypad code.
Date created	M	uint8[7]	The creation date. *Format:* | Year	uint16
---	---
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	

Request Keypad Codes (0x0043)

Name	Require ment	Format	Additional Information

Offset	M	uint16	The start offset to be read.
Count	M	uint16	The number of entries to be read, starting at the specified offset.
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Keypad Code Count (0x0044)

Name	Require ment	Format	Additional Information
Count	M	uint16	The total number of Keypad codes

Keypad Code (0x0045)

Name	Require ment	Format	Additional Information
Code ID	M	uint16	The id of this code.
Code	M	uint32	The code for this entry.
Name	M	uint8[20]	The name to be displayed for this

			entry.
Enabled	M	unit8	Flag indicating if this entry is enabled.
Date created	M	uint8[7]	The creation date. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Date last active	M	uint8[7]	The date of the last received request from this entry. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Lock count	M	uint16	The lock counter.
Time limited	M	uint8	Flag indicating if this entry is restricted to access only at certain

			times. The following fields are appended only if this flag is set.
Allowed from date	M	uint8[7]	The start timestamp from which access should be allowed. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Allowed until date	M	uint8[7]	The end timestamp until access should be allowed. *Format:* | Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8	
Allowed weekdays	M	uint8	Bitmask for allowed weekdays: `0 0 0 0 0 0 0` -- MO TU WE TH FR SA SU If no bit is set, all weekdays are allowed.

| Allowed from time | M | uint8[2] | The start time per day from which access should be allowed.

Format:

| Hour | uint8 |
Minute	uint8	
Allowed until time	M	uint8[2]	The end time per day until access should be allowed. *Format:* | Hour	uint8
Minute	uint8	

The Nuki Smart Lock will continue sending Keypad Code commands until the requested count is reached or no more entries are available.

Update Keypad Code (0x0046)

Name	Require ment	Format	Additional Information
Code ID	M	uint16	The id of the code to be updated.
Code	M	uint32	The code.
Name	M	uint8[20]	The name to be displayed for this authorization.
Enabled	M	unit8	Flag indicating if this entry is enabled.

Time limited	M	unit8	Flag indicating if this entry is restricted to access only at certain times.
Allowed from date	M	uint8[7]	The start timestamp from which access should be allowed *Format:* {{TABLE1}}
Allowed until date	M	uint8[7]	The end timestamp until access should be allowed *Format:* {{TABLE2}}
Allowed weekdays	M	uint8	Bitmask for allowed weekdays: `0 0 0 0 0 0 0` -- MO TU WE TH FR SA SU If no bit is set, all weekdays are

Format table (Allowed from date):

Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8

Format table (Allowed until date):

Year	uint16
Month	uint8
Day	uint8
Hour	uint8
Minute	uint8
Second	uint8

			allowed.
Allowed from time	M	uint8[2]	The start time per day from which access should be allowed. *Format:* | Hour	uint8
Minute	uint8	
Allowed until time	M	uint8[2]	The end time per day until access should be allowed. *Format:* | Hour	uint8
Minute	uint8	
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in [Security PIN handling](#).

Remove Keypad Code (0x0047)

Name	Requirement	Format	Additional Information
Code ID	M	uint16	The id of the code to be removed.
Nonce n K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16 uint32	The security pin, as defined in Security PIN handling.

Authorization Info (0x004C)

Name	Requirement	Format	Additional Information
Security PIN Info	M	uint8	Flag indicating if Security PIN is set. Only supported by Smart Lock Ultra.

Simple Lock Action (0x0100)

Name	Requirement	Format	Additional Information
Lock Action	M	uint8	The action to be executed. **0x01 unlock** **0x02 lock**
Name suffix	O	uint8[20]	Optional parameter containing a suffix which should be appended to the log entry.
Nonce n K	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

6. Error codes

General error codes

Code	Name	Usage
0xFD	ERROR_BAD_CRC	CRC of received command is invalid
0xFE	ERROR_BAD_LENGTH	Length of retrieved command payload does not match expected length

0xFF	ERROR_UNKNOWN	Used if no other error code matches

Pairing service error codes

P_ERROR_MAX_USER

Code	Name	Usage
0x10	P_ERROR_NOT_PAIRING	Returned if public key is being requested via request data command, but the Smart Lock is not in pairing mode
0x11	P_ERROR_BAD_AUTHEN TICATOR	Returned if the received authenticator does not match the own calculated authenticator
0x12	P_ERROR_BAD_PARAME TER	Returned if a provided parameter is outside of its valid range
0x13	P_ERROR_MAX_USER	Returned if the maximum number of users has been reached

Keyturner service error codes

Code	Name	Usage
0x20	K_ERROR_NOT_AUTHORIZ ED	Returned if the provided authorization id is invalid or the payload could not be decrypted using the shared key for this authorization id

0x21	K_ERROR_BAD_PIN	Returned if the provided pin does not match the stored one.
0x22	K_ERROR_BAD_NONCE	Returned if the provided nonce does not match the last stored one of this authorization id or has already been used before.
0x23	K_ERROR_BAD_PARAMET ER	Returned if a provided parameter is outside of its valid range.
0x24	K_ERROR_INVALID_AUTH_ ID	Returned if the desired authorization id could not be deleted because it does not exist.
0x25	K_ERROR_DISABLED	Returned if the provided authorization id is currently disabled.
0x26	K_ERROR_REMOTE_NOT_ ALLOWED	Returned if the request has been forwarded by the Nuki Bridge and the provided authorization id has not been granted remote access.
0x27	K_ERROR_TIME_NOT_ALL OWED	Returned if the provided authorization id has not been granted access at the current time.
0x28	K_ERROR_TOO_MANY_PIN _ATTEMPTS	Returned if an invalid pin has been provided too often
0x29	K_ERROR_TOO_MANY_EN TRIES	Returned if no more entries can be stored

0x2A	K_ERROR_CODE_ALREAD Y_EXISTS	Returned if a Keypad Code should be added but the given code already exists.
0x2B	K_ERROR_CODE_INVALID	Returned if a Keypad Code that has been entered is invalid.
0x2C	K_ERROR_CODE_INVALID_ TIMEOUT_1	Returned if an invalid pin has been provided multiple times.
0x2D	K_ERROR_CODE_INVALID_ TIMEOUT_2	Returned if an invalid pin has been provided multiple times.
0x2E	K_ERROR_CODE_INVALID_ TIMEOUT_3	Returned if an invalid pin has been provided multiple times.
0x40	K_ERROR_AUTO_UNLOCK _TOO_RECENT	Returned on an incoming auto unlock request and if an lock action has already been executed within short time.
0x41	K_ERROR_POSITION_UNK NOWN	Returned on an incoming unlock request if the request has been forwarded by the Nuki Bridge and the Smart Lock is unsure about its actual lock position.
0x42	K_ERROR_MOTOR_BLOCK ED	Returned if the motor blocks.
0x43	K_ERROR_CLUTCH_FAILU RE	Returned if there is a problem with the clutch during motor movement.
0x44	K_ERROR_MOTOR_TIMEO	Returned if the motor moves for a given period of time but did not

	UT	block.
0x45	K_ERROR_BUSY	Returned on any lock action via bluetooth if there is already a lock action processing.
0x46	K_ERROR_CANCELED	Returned on any lock action or during calibration if the user canceled the motor movement by pressing the button
0x47	K_ERROR_NOT_CALIBRAT ED	Returned on any lock action if the Smart Lock has not yet been calibrated
0x48	K_ERROR_MOTOR_POSITI ON_LIMIT	Returned during calibration if the internal position database is not able to store any more values
0x49	K_ERROR_MOTOR_LOW_V OLTAGE	Returned if the motor blocks because of low voltage.
0x4A	K_ERROR_MOTOR_POWE R_FAILURE	Returned if the power drain during motor movement is zero
0x4B	K_ERROR_CLUTCH_POWE R_FAILURE	Returned if the power drain during clutch movement is zero
0x4C	K_ERROR_VOLTAGE_TOO_ LOW	Returned on a calibration request if the battery voltage is too low and a calibration will therefore not be started
0x4D	K_ERROR_FIRMWARE_UP	Returned during any motor action if

	DATE_NEEDED	a firmware update is mandatory

7. Status codes

Code	Name	Usage
0x00	COMPLETE	Returned to signal the successful completion of a command
0x01	ACCEPTED	Returned to signal that a command has been accepted but the completion status will be signaled later.

8. List of timezone IDs

ID	Name	Offset	Timezone	DST
0	Africa/Cairo	UTC+2	EET	no
1	Africa/Lagos	UTC+1	WAT	no
2	Africa/Maputo	UTC+2	CAT, SAST	no
3	Africa/Nairobi	UTC+3	EAT	no
4	America/Anchorage	UTC-9/-8	AKDT	yes

5	America/Argentina/Buenos_Aires	UTC-3	ART, UYT	no
6	America/Chicago	UTC-6/-5	CDT	yes
7	America/Denver	UTC-7/-6	MDT	yes
8	America/Halifax	UTC-4/-3	ADT	yes
9	America/Los_Angeles	UTC-8/-7	PDT	yes
10	America/Manaus	UTC-4	AMT, BOT, VET, AST, GYT	no
11	America/Mexico_City	UTC-6/-5	CDT	yes
12	America/New_York	UTC-5/-4	EDT	yes
13	America/Phoenix	UTC-7	MST	no
14	America/Regina	UTC-6	CST	no
15	America/Santiago	UTC-4/-3	CLST, AMST, WARST, PYST	yes
16	America/Sao_Paulo	UTC-3	BRT	no
17	America/St_Johns	UTC-3½/-2½	NDT	yes

18	Asia/Bangkok	UTC+7	ICT, WIB	no
19	Asia/Dubai	UTC+4	SAMT, GET, AZT, GST, MUT, RET, SCT, AMT-Arm	no
20	Asia/Hong_Kong	UTC+8	HKT	no
21	Asia/Jerusalem	UTC+2/+3	IDT	yes
22	Asia/Karachi	UTC+5	PKT, YEKT, TMT, UZT, TJT, ORAT	no
23	Asia/Kathmandu	UTC+5¾	NPT	no
24	Asia/Kolkata	UTC+5½	IST	no
25	Asia/Riyadh	UTC+3	AST-Arabia	no
26	Asia/Seoul	UTC+9	KST	no
27	Asia/Shanghai	UTC+8	CST, ULAT, IRKT, PHT, BND, WITA	no
28	Asia/Tehran	UTC+3½	ARST	no
29	Asia/Tokyo	UTC+9	JST, WIT, PWT, YAKT	no

30	Asia/Yangon	UTC+6½	MMT	no
31	Australia/Adelaide	UTC+9½/ 10½	ACDT	yes
32	Australia/Brisbane	UTC+10	AEST, PGT, VLAT	no
33	Australia/Darwin	UTC+9½	ACST	no
34	Australia/Hobart	UTC+10/ +11	AEDT	yes
35	Australia/Perth	UTC+8	AWST	no
36	Australia/Sydney	UTC+10/ +11	AEDT	yes
37	Europe/Berlin	UTC+1/+ 2	CEST	yes
38	Europe/Helsinki	UTC+2/+ 3	EEST	yes
39	Europe/Istanbul	UTC+3	TRT	no
40	Europe/London	UTC+0/+ 1	BST, IST	yes
41	Europe/Moscow	UTC+3	MSK	no

42	Pacific/Auckland	UTC+12/ +13	NZDT	yes
43	Pacific/Guam	UTC+10	ChST	no
44	Pacific/Honolulu	UTC-10	H(A)ST	no
45	Pacific/Pago_Pago	UTC-11	SST	no
65535 (0xFF FF)	None			

9. Command usage examples

This section describes the usage of some basic commands to show the communication between the client (CL) and the Nuki Smartlock (SL).

Authorize App (Smart Lock 1 - 4th Generation)

1. User enables pairing mode on SL by pressing the button for 5 seconds
2. CL registers itself for indications on GDIO
3. CL writes Request Data command with Public Key command identifier to GDIO
   a. CL sends 0100030027A7
4. SL sends its public key via multiple indications on GDIO
   a. CL receives 0300DC040AFE6401550E1F7B20AB50135B80765834B9D898E6DA7129F61C62929B78A446
5. CL generates own keypair
   a. Private key C11CFB400A3A33414E89F9E6607271C2AF076405C5407984297F1DE0E7A54B73
   b. Public key F7A4FE9783C4C936A777963E78BB481533208D4E7D837373BA4B945747D9BA46
6. CL writes Public Key command to GDIO
   a. CL sends 0300F7A4FE9783C4C936A777963E78BB481533208D4E7D837373BA4B945747D9BA465694
7. Both sides calculate DH Key k using function dh1
   a. Key AB7D99698BF549F9AE80EA4D140D29D9B169C18533E5267D9E276F163B5C0B08
8. Both sides derive a long term shared secret key s from k using function kdf1
   a. Shared key 915561587D86815B709EDD5819D8C6F2E883DA3C86F461F13B84228B84533E04
9. SL sends Challenge command via multiple indications on GDIO
   a. CL receives 0400CC5F15190127A3B27D87160AE50D459B1530A50DD93E9D0C3DB05A6CFAA5D64A8A45
10. CL concatenates its own public key with SL's public key and the challenge to value r
11. CL calculates the authenticator a of r using function h1
12. SL calculates the same authenticator based on the already received information
13. CL writes Authorization Authenticator command with authenticator a to GDIO
    a. CL sends 05008D8163EF2E9F84BADE6BC3A5A5BAF613F8BF70F22C4DD7C514B8ECE932305FDBCCE5
14. SL verifies authenticator
15. SL sends Challenge command via multiple indications on GDIO
    a. CL receives

040070ACC47FBCC51C01378271565145C269005CF72CCD33768126B42D0DC5F942E6F7BA

16.   CL writes Authorization Data command to GDIO

    a.   CL writes 06008927B9AC416A5B1E367B58BC8D59C39E7FC8D0FD6DCC8F05863D34518CBAA2210027ED7E18546573746170700000000000000000000000000000000000000000000000000A72AE5BB4726C60FBB1AA28297081DCE45F76731711E39AC2B5FF9ACBDF03844C12C

17.   SL verifies authenticator
18.   SL stores new user and determines its authorization id
19.   SL sends Authorization-ID command via multiple indications on GDIO

    a.   CL receives 07006156B043406A20B4FCEF7E0684F4BDF4950420DD87FE855DB76306819A5B0CBAE05C34000177383DA0D13BD22354671DE3C7DF4FD3E6BD6162D21E61A313FF043AAD58C68652E338A4BF9FC7D99857B0DB85A3A9EA4C

    b.   Authorization-ID: 2

20.   CL verifies the received authenticator
21.   CL writes Authorization-ID Confirmation command to GDIO

    a.   CL sends 1E00D36427B554B2394AA96F99F524B189E0A312B65226E929B7E7C76F4D4D197072E05C34007BF4

22.   SL sends Status COMPLETE via multiple indications on GDIO

    a.   CL receives 0E00009DD7

Authorize App (Smart Lock Ultra)

1.   User enables pairing mode on SL by pressing the button for 5 seconds
2.   CL registers itself for indications on GDIO
3.   CL writes Request Data command with Public Key command identifier to GDIO

    b.   CL sends 0100030027A7

5.   SL sends its public key via multiple indications on GDIO

    b.   CL receives 03002796E928F26EA02AC44D0A12A3C85863EC2DD3CFE238DB153CA7F7F05797737D49CE

6.   CL generates own keypair

    c.   Private key 9C9A0BE17339C58380237220BE8D91F5EC3FA7317B5CBB3DD2E051E226F4E2CD

    d.   Public key CAD42392DE77329DD8B130419D7B86D228D1901B5DD618C375E6864EF9446328

7.   CL writes Public Key command to GDIO

    b.   CL sends 0300CAD42392DE77329DD8B130419D7B86D228D1901B5DD618C375E6864EF94463283E4D

8.   Both sides calculate DH Key k using function dh1

    b.   Key AB7D99698BF549F9AE80EA4D140D29D9B169C18533E5267D9E276F163B5C0B08

9.   Both sides derive a long term shared secret key s from k using function kdf1

b.   Shared key
915561587D86815B709EDD5819D8C6F2E883DA3C86F461F13B84228B84533E04
10.   SL sends Challenge command via multiple indications on GDIO
b.   CL receives
0400DC9310E28331B8B38392ABD0915E0CD4A28DABD905F20E3747E12678A941E
BD9756D
14.   CL concatenates its own public key with SL's public key and the challenge to value r
15.   CL calculates the authenticator a of r using function h1
16.   SL calculates the same authenticator based on the already received information
17.   CL writes Authorization Authenticator command with authenticator a to GDIO
b.   CL sends
050006D99C56E63679964A6C2A60E692F4E1B7BC13B1216F052B0F65BD007BDB90
EDE02C
16.   SL verifies authenticator
17.   SL sends Authorization Info command via multiple indications on GDIO
b.   CL receives
4C000050A4
17.   CL writes Authorization Data command to GDIO, encrypting the data with the calculated
shared key and the Authorization-ID set to 0x7FFFFFFF
b.   CL writes
06000000000054657374461707000000000000000000000000000000000000000000
00000040E20100
20.   SL verifies authenticator
21.   SL stores new user and determines its authorization id
22.   SL sends Authorization-ID command via multiple indications on GDIO
c.   CL receives following encrypted payload
0700F88700008127D49A5F985C4483884720B3061453BB4E
d.   Authorization-ID: 34808

Read lock state

Authorization-ID: 2

1.   CL writes [Request Data](#) command with [Keyturner States](#) command identifier to USDIO
a.   Unencrypted: 0200000001000C00418D
b.   Encrypted:
37917F1AF31EC5940705F34D1E5550607D5B2F9FE7D496B6020000001A00670D124926004
366532E8D927A33FE84E782A9594D39157D065E
c.   CL sends encrypted message
2.   SL sends [Keyturner States](#) command via multiple indications on USDIO
a.   CL receives 90B0757CFED0243017EAF5E089F8583B9839D61B
b.   CL receives 050924D2020000002700B13938B67121B6D528E7
c.   CL receives DE206B0D7C5A94587A471B33EBFB012CED8F1261
d.   CL receives 135566ED756E3910B5
e.   Decrypted: 020100E0070307080F1E3C0000200A
i.   Nuki state: 02
ii.   Lock state: 01
iii.   Lock trigger: 00
iv.   Time: 2016-03-07 08:15:30
v.   Offset: 60
vi.   Battery critical: false

Perform unlock

Shared key:
217FCB0F18CAF284E9BDEA0B94B83B8D10867ED706BFDEDBD2381F4CB3B8F730

Authorization-ID: 2

1.   CL writes Request Data command with Challenge command identifier to USDIO
a.   Unencrypted: 020000001000400E804
b.   Encrypted:
88FDEFD7F941B63C242B7F84B3D786886340A4A8B1C1EAA0020000001A00066819A2956E
6A79AF6ED66D257B276715F51F63A8BEB9ED0D47
c.   CL sends encrypted message
2.   SL sends Challenge command via multiple indications on USDIO
a.   CL receives 99C8613A9F6AB6D3FB0399D37AD38C5C003AC139
b.   CL receives B1567BC102000000380028CDCbackground-lightgreen8C08DA47BF32
c.   CL receives 3BF9371EBF068F6D480438563660780A4234D9A2
d.   CL receives 3794E305EE37878874EDE106A0BBFCF5B60E0C2E
e.   CL receives 2BA17248A02B
f.   Decrypted:
57D95521BEA186B5A9244F025737924C5B7E33592D0614D5F6EF2E2F142C6D4B
3.   CL writes Lock Action command with action 0x01 to USDIO
a.   Unencrypted:
020000000D0001000000000057D95521BEA186B5A9244F025737924C5B7E33592D0614D5F
6EF2E2F142C6D4BCACF
b.   Encrypted:
19467990B69FFBE3D484A5882C995449E3EBC878712152E7020000003E00B30D19E0C0A1
2F4D8C887864877B8853437825D587F85BB6C21BF674E204A685AC5E40E8A5FDB85349F5
20069496F092FAB63736928C0933DB34CFA21809
c.   CL sends encrypted message
4.   SL send Status ACCEPTED via multiple indications on USDIO
a.   CL receives 020000000E00010D9A
5.   SL sends Keyturner States command with status unlocking on USDIO
a.   CL receives decrypted: 020200E00703070818203C00000007
6.   SL sends Keyturner States command with status unlocked on USDIO
a.   CL receives decrypted: 020300E007030708182C3C00000007
7.   SL sends Status COMPLETE via multiple indications on USDIO
a.   CL receives 020000000E00002C8A

10. Changelog

Changelog v.2.3.0

08.01.2025

Updated:

Added support for Smart Lock Ultra

Changelog v.2.2.2

22.01.2024

Updated:

Corrected description and information of the "Authorize App" flow.

Changelog v.2.2.1

22.06.2021

1. Update the information regarding the Keyturner Service MTU size.
2. Corrected information about how to set "Auto Lock" option in Advanced Config to false for current firmware version.

Changelog v.2.2.0

08.10.2020

New:

Added the Critical Battery State in 0x000C: Keyturner States

Added the new Accessory Battery State to 0x000C: Keyturner States

Updated:

Updated the new Accessory Battery State in 0x000C: Keyturner States

Changelog v.2.1.0

28.01.2020

New:

0x0100: Simple Lock Action

Updated:

Added the new nightmode settings to 0x0035: Set Advanced Config and 0x0037: Advanced Config

Fixed several formatting issues

Changelog v.2.0.0

12.11.2018

New:

0x0041 - 0x0048: Keypad commands

0x003A - 0x003F: Time control commands

0x0031 - 0x0034: Reworked log commands

Updated:

0x000C: Updated Smart Lock states for scheduled events, auto-lock and the door sensor

0x0011: Added more details to the battery report command

0x0015: Added Homekit status

0x000C, 0x0013, 0x0015: Added Timezone support

Error codes: More detailed error codes available

Removed:

0x0022 - 0x0026: Replaced log commands