NUKI

SMARTLOCK API

V1.10

20.11.2017

Nuki Home Solutions GmbH
Münzgrabenstraße 92/4 • 8010 Graz • Austria • contact@nuki.io • T +43 316 22 84 09 • F +43 316 22 84 12 50

Introduction

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

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 KT.

Keyturner Pairing Service

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

General Data Input Output characteristic

The General Data Input Output characteristic is used to send data to or retrieve data from the Nuki KT. 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 KT 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 KT. 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 KT by using the GATT Write (Long) Characteristic Value sub-procedure.

Value
UUID: a92ee201-5501-11e4-916c-0800200c9a66
Type: uint8 array (max size is 20 Bytes)
Properties: write (long), indicate

Client configuration
Properties: write

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 KT. 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 KT 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

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

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

Commands

Command identifier	Command
0x0001	Request Data
0x0003	Public Key
0x0004	Challenge
0x0005	Authorization Authenticator
0x0006	Authorization Data
0x0007	Authorization-ID
0x0008	Remove User Authorization
0x0009	Request Authorization Entries
0x000A	Authorization Entry
0x000B	Authorization Data (Invite)
0x000C	Nuki 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 User Authorization
0x0027	Authorization Entry Count
0x0030	Request Disconnect
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

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.

Request Data (0x0001)

Name	Requirement	Format	Additional Information
Command identifier	M	uint16	The identifier of the command to be executed by the Nuki Smartlock.
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 n_K	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 Nuki Smartlock.
Nonce n_{K}	M	uint8[32]	An arbitrary number used only once to resist replay attacks. (unpredictable, probabilistic non-reuse)

Authorization Data (0x0006)

Name	Requirement	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
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[3	An arbitrary number used only

		2]	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)

Authorization-ID (0x0007)

Name	**Requirement**	**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.
UUID	M	uint8[16]	Random identifier unique per Nuki Smartlock and not altered until Nuki Smartlock 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)

Authorization-ID Confirmation (0x001E)

Name	**Requirement**	**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	**Requirement**	**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	unit16	The security pin.

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.
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Authorization Entry (0x000A)

Name	Requirement	Format	Additional Information
Authorization-ID	M	uint32	The Authorization-ID.
ID Type	M	uint8	The type of the ID.
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 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	unit8	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 Smartlock 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	**Requirement**	**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.
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. *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	The security pin.

Authorization-ID (Invite) (0x001F)

Name	**Requirement**	**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	**Requirement**	**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	The security pin.

Nuki States (0x000C)

Name	**Requirement**	**Format**	**Additional Information**

Nuki State	M	uint8	The current operation state of the Nuki Smartlock 0x00 Uninitialized 0x01 Pairing Mode 0x02 Door Mode
Lock State	M	uint8	The current state of the locking mechanism within Nuki Smartlock 0x00 uncalibrated 0x01 locked 0x02 unlocking 0x03 unlocked 0x04 locking 0x05 unlatched 0x06 unlocked (lock ‘n’ go active) 0x07 unlatching 0xFE motor blocked 0xFF undefined
Trigger	M	uint8	The trigger, that caused the state change of the unlock mechanism within Nuki Smartlock 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 Smartlocks button
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. 0x00 ok 0x01 critical
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

Lock Action (0x000D)

Name	**Requirement**	**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

			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: 0 0 0 0 0 0 0 0 -- -- -- -- -- -- FC AU AU Auto Unlock FC Force Unlock Other bits are reserved for future use.
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**
Command identifier	M	uint16	The identifier of the most recently executed command by the Nuki Smartlock.

Openings Closings Summary (0x0010)

Name	Requirement	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 Nuki Smartlock booted
Closings since boot	M	uint16	The number of closings since the Nuki Smartlock booted

Battery Report (0x0011)

Name	Requirement	Format	Additional Information
Battery Drain	M	uint16	The current battery drain in Milliamperes (mA).
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

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 Nuki Smartlock.
Latitude	M	float	The latitude of the Nuki Smartlock's geoposition.
Longitude	M	float	The longitude of the Nuki Smartlock's 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 Smartlock 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.
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Request Config (0x0014)

Name	**Requirement**	**Format**	**Additional Information**

Nonce n_K	M	uint8[32]	The nonce received from the challenge.

Config (0x0015)

Name	Requirement	Format	Additional Information
Nuki-ID	M	uint32	The unique identifier of the Nuki Smartlock.
Name	M	uint8[32]	The name of the Nuki Smartlock.
Latitude	M	float	The latitude of the Nuki Smartlock's geoposition.
Longitude	M	float	The longitude of the Nuki Smartlock's 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.

Set Security PIN (0x0019)

Name	Requirement	Format	Additional Information
PIN	M	uint16	The new security pin.
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Verify Security PIN (0x0020)

Name	Requirement	Format	Additional Information
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Request Calibration (0x001A)

Name	Requirement	Format	Additional Information
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Request Reboot (0x001D)

Name	Requirement	Format	Additional Information
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Update Time (0x0021)

Name	Requirement	Format	Additional Information
Time	M	uint8[7]	Timestamp *Format:* Year uint16 Month uint8 Day uint8 Hour uint8 Minute uint8 Second uint8
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Authorization Entry Count (0x0027)

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

Request Disconnect (0x0030)

Name	Requirement	Format	Additional Information
No payload			

Request Log Entries (0x0031)

Name	Requirement	Format	Additional Information
Start index	M	uint32	The index where to start reading log entries. *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	The security pin.

Log Entry (0x0032)

Name	Requirement	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
Data	M	uint8[x]	*Type 0x01:* x = 1 0x00 Logging disabled 0x01 Logging enabled *Type 0x02:* x = 4 byte 1: Lock Action byte 2: Trigger byte 3: Auto-Unlock Flag byte 4: Completion status 0x00 ... Success 0x01 ... Motor blocked 0x02 ... Canceled 0x03 ... Too recent 0x04 ... Busy 0x05 ... Low motor voltage 0x06 ... Clutch failure 0x07 ... Motor power failure 0xFE ... Other error 0xFF ... UNKNOWN

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

Log Entry Count (0x0033)

Name	Requi	Format	Additional Information

	reme nt		
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*

Enable Logging (0x0034)

Name	**Requir ement**	**Forma t**	**Additional Information**
Enabled	M	uint8	Flag indicating if logging should be enabled.
Nonce n_K	M	uint8[3 2]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Set Advanced Config (0x0035)

Name	**Requir ement**	**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 Nuki Smartlock 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 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.
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

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	M	uint8	The desired action, if the button is

action			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 Nuki Smartlock 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.

Add Time Control Entry (0x0039)

Name	Requirement	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 used.
Time	M	uint8[2]	*Format:* Hour uint8 Minute uint8
Lock action	M	uint8	The desired lock action See Lock Action
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Time Control Entry ID (0x003A)

Name	Requirement	Format	Additional Information
Entry ID	M	uint8	The unique identifier of the recently created time control entry.

Remove Time Control Entry (0x003B)

Name	Requirement	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	The security pin.

Request Time Control Entries (0x003C)

Name	Requirement	Format	Additional Information
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

Time Control Entry Count (0x003D)

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

Time Control Entry (0x003E)

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 0 -- MO TU WE TH FR SA SU If no bit is set, all weekdays are used.
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 0 -- MO TU WE TH FR SA SU If no bit is set, all weekdays are used.
Time	M	uint8[2]	*Format:* Hour uint8 Minute uint8
Lock action	M	uint8	The desired lock action See Lock Action
Nonce n_K	M	uint8[32]	The nonce received from the challenge.
Security-PIN	M	uint16	The security pin.

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

Code	Name	Usage
0x10	P_ERROR_NOT_PAIRING	Returned if public key is being requested via request data command, but Smartlock is not in pairing mode
0x11	P_ERROR_BAD_AUTHENTICATOR	Returned if the received authenticator does not match the own calculated authenticator
0x12	P_ERROR_BAD_PARAMETER	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_AUTHORIZED	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_PARAMETER	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_ALLOWED	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
0x40	K_ERROR_AUTO_UNLOCK_TOO_RECENT	Returned on an incoming auto unlock request and if an auto unlock has already been executed within short time
0x41	K_ERROR_POSITION_UNKNOWN	Returned on an incoming unlock request if the request has been forwarded by the Nuki Bridge and the Smartlock is unsure about its actual lock position
0x42	K_ERROR_MOTOR_BLOCKED	Returned if the motor blocks
0x43	K_ERROR_CLUTCH_FAILURE	Returned if there is a problem with the clutch during motor movement
0x44	K_ERROR_MOTOR_TIMEOUT	Returned if the motor moves for a given period of time but did not block
0x45	K_ERROR_BUSY	Returned on any lock action via bluetooth if there is already a lock action processing

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

Nuki Home Solutions GmbH
Münzgrabenstraße 92/4 • 8010 Graz • Austria • contact@nuki.io • T +43 316 22 84 09 • F +43 316 22 84 12 50

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

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 03002FE57DA347CD62431528DAAC5FBB290730FF
    b. CL receives F684AFC4CFC2ED90995F58CB3B749DB9
5. CL generates own keypair
    a. Private key 8CAA54672307BFFDF5EA183FC607158D2011D008ECA6A1088614FF0853A5AA07
    b. Public key F88127CCF48023B5CBE9101D24BAA8A368DA94E8C2E3CDE2DED29CE96AB50C15
6. CL writes Public Key command to GDIO
    a. CL sends 0300F88127CCF48023B5CBE9101D24BAA8A368DA94E8C2E3CDE2DED29CE96AB50C159241
7. Both sides calculate DH Key *k* using function dh1
    a. Key 0DE40B998E0E330376F2D2FC4892A6931E25055FD09F054F99E93FECD9BA611E
8. Both sides derive a long term shared secret key *s* from *k* using function kdf1
    a. Shared key 217FCB0F18CAF284E9BDEA0B94B83B8D10867ED706BFDEDBD2381F4CB3B8F730
9. SL sends Challenge command via multiple indications on GDIO
    a. CL receives 04006CD4163D159050C798553EAA57E278A579AF
    b. CL receives FCBC56F09FC57FE879E51C42DF17C3DF
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 0500B09A0D3979A029E5FD027B519EAA200BC14AD3E163D3BE4563843E021073BCB1C357
14. SL verifies authenticator
15. SL sends Challenge command via multiple indications on GDIO
    a. CL receives 0400E0742CFEA39CB46109385BF91286A3C02F40
    b. CL receives EE86B0B62FC34033094DE41E2C0D7FE1
16. CL writes Authorization Data command to GDIO
    a. CL writes 0600CF1B9E7801E3196E6594E76D57908EE500AAD5C33F4B6E0BBEA0DDEF82967BFC00000000004D617263202854657374290000000000000000000000000000000000000000052AFE0A664B4E9B56DC6BD4CB718A6C9FED6BE17A7411072AA0D31537814057769F2
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 07003A270A2E453443C3790E657CEBE634B03F01
    b. CL receives 02F45681B4067C661D46E6E15EDF0200000083B3
    c. CL receives 3643C6D97EF77ED51C02A277CBF7EA479915982F
    d. CL receives 13C61D997A56678AD77791BFA7E95229A3DD34F8
    e. CL receives 7132BF3E3C97DB9F
    f. Authorization-ID: 2
20. CL verifies the received authenticator
21. CL writes Authorization-ID Confirmation command to GDIO
    a. CL sends 1E003A41B91A66FBC4D22EFEFBB7272140829695A3917433D5BEB981B76166D13F8A02000000CDF5
22. SL sends Status COMPLETE via multiple indications on GDIO
    a. CL receives 0E00009DD7

Read lock state

Shared key: 217FCB0F18CAF284E9BDEA0B94B83B8D10867ED706BFDEDBD2381F4CB3B8F730
Authorization-ID: 2

1. CL writes Request Data command with Nuki States command identifier to USDIO

    a. Unencrypted: 02000000010000C00418D
    b. Encrypted: 37917F1AF31EC5940705F34D1E5550607D5B2F9FE7D496B602000000001A00670D124926004366532E8D927A33FE84E782A9594D39157D065E
    c. CL sends encrypted message
2. SL sends Nuki 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: 0200000001000400E804
    b. Encrypted: 88FDEFD7F941B63C242B7F84B3D786886340A4A8B1C1EAA0020000001A00066819A2956E6A79AF6ED66D257B276715F51F63A8BEB9ED0D47
    c. CL sends encrypted message
2. SL sends Challenge command via multiple indications on USDIO
    a. CL receives 99C8613A9F6AB6D3FB0399D37AD38C5C003AC139
    b. CL receives B1567BC102000000380028CDCC668C08DA47BF32
    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:

020000000D000100000000000 57D95521BEA186B5A9244F0257 37924C5B7E33592D0614D5F6EF2E2F142C6D4B CACF

   b. Encrypted: 19467990B69FFBE3D484A5882C995449E3EBC878712152E702 0000003E00B30D19E0C0A12F4D8C887864877B8853437825D5 87F85BB6C21BF674E204A685AC5E40E8A5FDB85349F5200694 96F092FAB63736928C0933DB34CFA21809
   c. CL sends encrypted message
4. SL send Status ACCEPTED via multiple indications on USDIO
   a. CL receives 020000000E00010D9A
5. SL sends Nuki States command with status *unlocking* on USDIO
   a. CL receives decrypted: 020200E007030708182O3C00000007
6. SL sends Nuki 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 020000000E000002C8A