YKOATH Protocol Specification

The YKOATH protocol is used to manage and use OATH credentials with a YubiKey NEO or a YubiKey 4. It can be accessed over USB (when the CCID transport is enabl or over NFC, using ISO 7816-4 commands as defined in this document.

General Definitions

Instructions

Instructions marked as *Require Auth* require a successful VALIDATE command to be performed before they are available, if a validation code is set.

Name	**Code**	**Require Auth**
PUT	0x01	Y
DELETE	0x02	Y
SET CODE	0x03	Y
RESET	0x04	N
LIST	0xa1	Y
CALCULATE	0xa2	Y
VALIDATE	0xa3	N
CALCULATE ALL	0xa4	Y
SEND REMAINING	0xa5	Y

ALGORITHMS

HMAC-SHA1	0x01
HMAC-SHA256	0x02
HMAC-SHA512	0x03

NoteHMAC-SHA512 requires YubiKey 4.3.1 or later.

TYPES

HOTP	0x10
TOTP	0x20

PROPERTIES

Only increasing	0x01	Enforces that a challenge is always higher than th previous
Require touch	0x02	Require button press to generate OATH codes

NoteRequire touch requires YubiKey 4.2.4 or later.

SELECT INSTRUCTION

Selects the application for use and returns version, ID and a challenge if authentication is configured (see the validate instruction below).

Request Syntax

CLA	0x00
INS	0xa4
P1	0x04
P2	0x00
Lc	Length of AID (7)
Data	AID (0xa0 0x00 0x00 0x05 0x27 0x21 0x01)

Response Syntax

A challenge is returned if the authentication object is set. In that case an authentication is required for all commands except VALIDATE and RESET.

Version tag	0x79
Version length	Length of version
Version data	Version
Name tag	0x71
Name length	Length of name
Name data	Name
Challenge tag	0x74
Challenge length	Length of challenge
Challenge data	Challenge
Algorithm tag	0x7b
Algorithm length	Length of algorithm (1)
Algorithm	What algorithm to use

PUT INSTRUCTION

Adds a new (or overwrites) OATH credential.

Request Syntax

CLA	0x00
INS	0x01
P1	0x00

P2	0x00
Lc	Length of Data
Data	Put Data

Put Data

Name tag	0x71
Name length	Length of name data, max 64 bytes
Name data	Name
Key tag	0x73
Key length	Length of key data + 2
Key algorithm	High 4 bits is type, low 4 bits is algorithm
Digits	Number of digits in OATH code
Key data	Key
Property tag(o)	0x78
Property(o)	Property byte
IMF tag(o)	0x7a (only valid for HOTP)
IMF length(o)	Length of imf data
IMF data(o)	Imf

Response Codes

Success	0x9000
No space	0x6a84
Auth required	0x6982
Wrong syntax	0x6a80

DELETE INSTRUCTION

Deletes an existing credential.

Request Syntax

CLA	0x00
INS	0x02
P1	0x00

P2	0x00
Lc	Length of Data
Data	Delete Data

Delete Data

Name tag	0x71
Name length	Length of name data
Name data	Name

Response Codes

Success	0x9000
No such object	0x6984
Auth required	0x6982
Wrong syntax	0x6a80

SET CODE INSTRUCTION

Configures Authentication. If length 0 is sent, authentication is removed. The key to be set is expected to be a user-supplied UTF-8 encoded password passed through 1 rounds of PBKDF2 with the ID from select used as salt. 16 bytes of that are used. When configuring authentication you are required to send a challenge and one authentication-response with that key, in order to confirm that the application and the host software can calculate the same response for that key.

Request Syntax

CLA	0x00
INS	0x03
P1	0x00
P2	0x00
Lc	Length of Data
Data	Set Code Data

Set Code Data

Key tag	0x73
Key length	Length of key data + 1
Key algorithm	Algorithm
Key data	Key
Challenge tag	0x74

Challenge length	Length of challenge data
Challenge data	Challenge
Response tag	0x75
Response length	Length of response data
Response data	Response

Response Codes

Success	0x9000
Response doesn’t match	0x6984
Auth required	0x6982
Wrong syntax	0x6a80

RESET INSTRUCTION

Resets the application to just-installed state.

Request Syntax

CLA	0x00
INS	0x04
P1	0xde
P2	0xad

Response Codes

Success	0x9000

LIST INSTRUCTION

Lists configured credentials.

Request Syntax

CLA	0x00
INS	0xa1
P1	0x00
P2	0x00

Response Syntax

Response will be a continual list of objects looking like:

Name list tag	0x72
Name length	Length of name + 1
Algorithm	High 4 bits is type, low 4 bits is algorithm
Name data	Name

Response Codes

Success	0x9000
More data available	0x61xx
Auth required	0x6982
Generic error	0x6581

CALCULATE INSTRUCTION

Performs CALCULATE for one named credential.

Request Syntax

CLA	0x00
INS	0xa2
P1	0x00
P2	0x00 for full response 0x01 for truncated
Lc	Length of data
Data	Calculate data

Calculate Data

Name tag	0x71
Name length	Length of name data
Name data	Name
Challenge tag	0x74
Challenge length	Length of challenge
Challenge data	Challenge

Response Syntax

Response tag	0x75 for full response, 0x76 for truncated
Response length	Length of response + 1

Digits	Number of digits in the OATH code
Response data	Response

Response Codes

Success	0x9000
No such object	0x6984
Auth required	0x6982
Wrong syntax	0x6a80
Generic error	0x6581

VALIDATE INSTRUCTION

Validates authentication (mutually). The challenge for this comes from the SELECT command. The response if computed by performing the correct HMAC function of challenge with the correct key. A new challenge is then sent to the application, together with the response. The application will then respond with a similar calculatio the host software can verify.

Request Syntax

CLA	0x00
INS	0xa3
P1	0x00
P2	0x00
Lc	Length of data
Data	Validate data

Validate Data

Response tag	0x75
Response length	Length of response
Response data	Response
Challenge tag	0x74
Challenge length	Length of challenge
Challenge data	Challenge

Response Syntax

Response tag	0x75
Response length	Length of response

Response data	Response

Response Codes

Success	0x9000
Auth not enabled	0x6984
Wrong syntax	0x6a80
Generic error	0x6581

CALCULATE ALL INSTRUCTION

Performs CALCULATE for all available credentials, returns name + response for TOTP and just name for HOTP and credentials requiring touch.

Request Syntax

CLA	0x00
INS	0xa4
P1	0x00
P2	0x00 for full response 0x01 for truncated
Lc	Length of data
Data	Calculate all data

Calculate All Data

Challenge tag	0x74
Challenge length	Length of challenge
Challenge data	Challenge

Response Syntax

For HOTP the response tag is 0x77 (No response) For credentials requiring touch the response tag is 0x7c (No response) The response will be a list of the following obj

Name tag	0x71
Name length	Length of name
Name data	Name
Response tag	0x77 for HOTP, 0x7c for touch, 0x75 for full response or 0x76 for truncated response
Response len	Length of response + 1
Digits	Number of digits in the OATH code
Response data	Response

Response Codes

Success	0x9000
More data available	0x61xx
Auth required	0x6982
Wrong syntax	0x6a80
Generic error	0x6581

SEND REMAINING INSTRUCTION

Gets remaining data if everything didn’t fit in previous response (response code was 61xx).

Request Syntax

CLA	0x00
INS	0xa5
P1	0x00
P2	0x00

Response Syntax

Data	Continued data where previous command left off