

Yubikey felprogramozása a GreenRADIUS-hoz, OATH HOTP módban

1. BEVEZETŐ

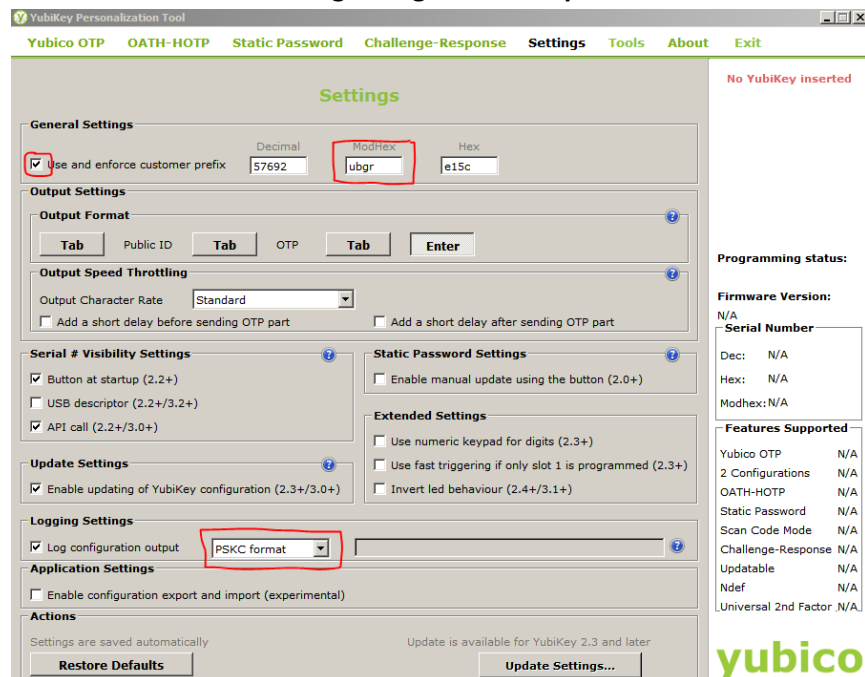
Ez a leírás bemutatja, hogyan programozzuk fel a Yubikey kulcsokat OATH HOTP módban. Az így létrejövő OTP - egyszer használatos jelszó - 18 karakter lesz az alapértelmezett 44 karakter helyett.

2. ELŐFELTÉTELEK

- Legyen nálunk az összes Yubikey amit fel akarunk programozni.
- Töltsük le és telepítsük fel a Yubico Personalization Tool-t a gépünkre ([letölthető innen](#))
- Amennyiben további Yubikey kulcsokra van szükségünk, akkor azok [itt vásárolhatók](#) meg.

3. YUBIKEY KULCSOK FELPROGRAMOZÁSA

1. Nyissuk meg a **Yubico Personalization Tool**-t
2. Válasszuk ki a **"Settings"** menüpontot
 - a. Kattintsuk be "Use and enforce customer prefix"-t és a ModHex mezőbe írjuk be, hogy "ubgr"
 - b. Válasszuk ki a **"PSKC"** a **"Log configuration output"** részben.



Yubico Personalization Tool

Yubico OTP OATH-HOTP Static Password Challenge-Response **Settings** Tools About Exit

Settings

No YubiKey inserted

General Settings

Use and enforce customer prefix

Decimal: 57692 ModHex: **ubgr** Hex: e15c

Output Settings

Output Format

Tab Public ID Tab OTP Tab Enter

Output Speed Throttling

Output Character Rate: Standard

Add a short delay before sending OTP part Add a short delay after sending OTP part

Serial # Visibility Settings

Button at startup (2.2+)

USB descriptor (2.2+/3.2+)

API call (2.2+/3.0+)

Static Password Settings

Enable manual update using the button (2.0+)

Extended Settings

Use numeric keypad for digits (2.3+)

Use fast triggering if only slot 1 is programmed (2.3+)

Invert led behaviour (2.4+/3.1+)

Update Settings

Enable updating of YubiKey configuration (2.3+/3.0+)

Logging Settings

Log configuration output

PSKC format

Application Settings

Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

Restore Defaults Update Settings...

Programming status:

Firmware Version:

N/A

Serial Number:

Dec: N/A

Hex: N/A

Modhex: N/A

Features Supported

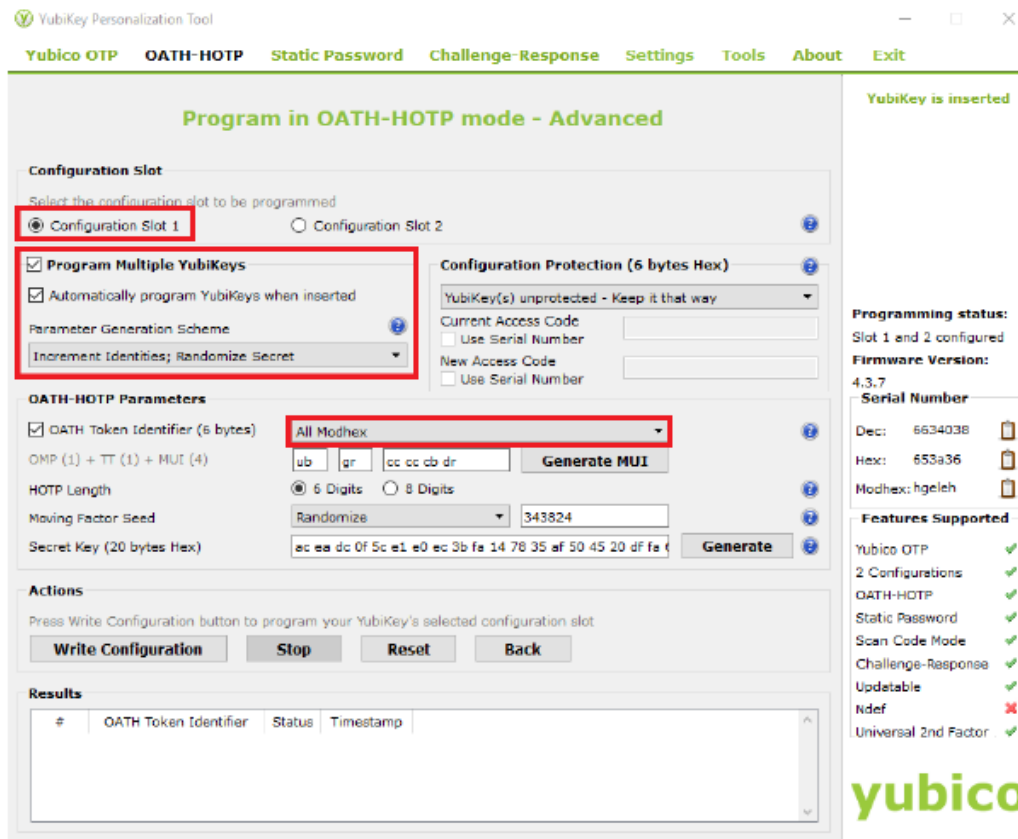
Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

yubico

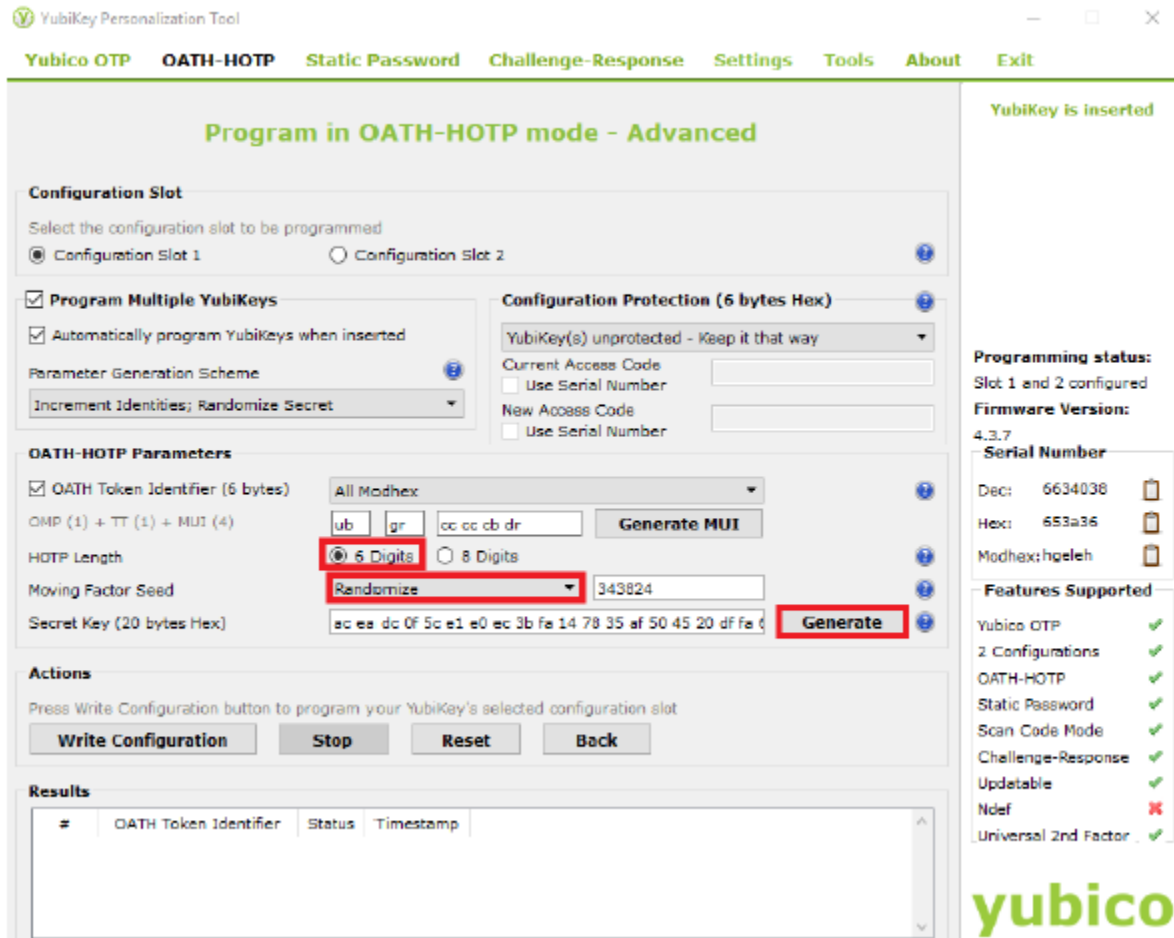
3. Válasszuk ki a "OATH-HOTP" menüpontot és kattintsunk az "Advanced" gombra.



4. A következő képet fogod látni lásd alább:
- Válasszuk ki a "Configuration Slot 1"-t
 - Válasszuk ki a "Program Multiple Yubikeys"-t
 - Válasszuk ki a "Select Automatically program YubiKeys when inserted"-t
 - A "Under Parameter Generation Scheme" alatt válasszuk ki a "Increment Identities; Randomize Secret" opciót.
 - Az OATH-HOTP Parameters alatt válasszuk ki az "All Modhex"-t



- Állítsuk be a HOTP hosszát "6 digits"-re, valamint a "Moving Factor Seed"-t "Randomize"-re majd kattintsunk a "Generate" gombra, hogy



YubiKey Personalization Tool

Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Tools About Exit

Program in OATH-HOTP mode - Advanced

Configuration Slot
Select the configuration slot to be programmed
 Configuration Slot 1 Configuration Slot 2

Program Multiple YubiKeys
 Automatically program YubiKeys when inserted
 Parameter Generation Scheme: Increment Identities; Randomize Secret

Configuration Protection (6 bytes Hex)
 YubiKey(s) unprotected - Keep it that way
 Use Serial Number
 Current Access Code:
 New Access Code:
 Use Serial Number

OATH-HOTP Parameters
 OATH Token Identifier (6 bytes) All Modhex
 OMP (1) + TT (1) + MUI (4) ub gr cc cc cb dr **Generate MUI**
 HOTP Length: 6 Digits 8 Digits
 Moving Factor Seed: Randomize 343824
 Secret Key (20 bytes Hex): ac ea dc 0f 5c e1 e0 ec 3b fa 14 78 35 af 50 45 20 df fa **Generate**

Actions
 Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	OATH Token Identifier	Status	Timestamp

YubiKey is inserted

Programming status:
Slot 1 and 2 configured

Firmware Version:
4.3.7

Serial Number

Dec: 6634038
 Hex: 653a36
 Modhex: hgeleh

Features Supported

- Yubico OTP ✓
- 2 Configurations ✓
- OATH-HOTP ✓
- Static Password ✓
- Scan Code Mode ✓
- Challenge-Response ✓
- Updatable ✓
- Ndef ✗
- Universal 2nd Factor ✓

yubico

- Helyezzük be az első Yubikey és kattintsunk a "Write Configuration" gombra. Nevezzük el a kimeneti fájlt és mentjük el. (Megjegyzés: biztosítsuk, hogy a kimeneti fájl ne tartalmazzon szóköz karaktereket.) Ez a fájl fogja tartalmazni a felprogramozott Yubikey kulcsok biztonsági adatait. Kérjük tartsa biztonságos helyen addig amíg nem töltjük be a GreenRADIUS-ba.
- A már behelyezett Yubikey felprogramozásra kerül és ebben az esetben annak sikerességéről szóló üzenetet kapunk. Távolítsuk el a Yubikey-t.
- Anélkül, hogy kilépnénk az alkalmazásból, helyezzük be a következő Yubikey-t. Várjuk meg, hogy a program a behelyezett Yubikey-t felprogramozza (a sikerességről üzenetet kapunk), majd távolítsuk el. Folytassuk ezt a folyamatot a maradék Yubikey kulcsokkal.
- Miután minden Yubikey-t felprogramoztunk, kattintsunk a "Stop" gombra és csukjuk be az alkalmazást.

4. AZ ÚJ TITOK FÁJL IMPORTÁLÁSA A GREENRADIUSBA

- Nyissunk meg egy új ablakot a böngészőben és menjünk a GreenRADIUS adminisztrációs weboldalára.
- Győződjünk meg arról, hogy az ellenőrzést végző szervert "Local Validation Server on GreenRADIUS"-re van beállítva. Ezt a "Global Configuration" fül alatt a "Validation Server"-nél állíthatjuk be.

3. Szintén a "Global Configuration" alatt a "General settings"-be állítsuk be "YubiKey (OATH-HOTP Mode) Configuration – OTP Length" 6-ra és mentjük el a "Save" gombbal.
4. Menjünk az "Import Secrets" menüpontra.
5. Válasszuk ki a "Import OATH Tokens (PSKC Container)"-t és kattintsunk a "Browse..." gombra.
6. Válasszuk ki a felprogramozáskor létrehozott fájlt.
7. Kattintsunk az "Upload" gombra. Ne menjünk el a weboldalról. Várja meg a sikerességet megjelenítő üzenetet.
8. Miután a feltöltés sikerült, az újonnan importált tokeneket a "List Tokens" fül alatt láthatjuk.