

Programovanie Yubikey pre GreenRADIUS, v režime OATH HOTP

1. ÚVOD

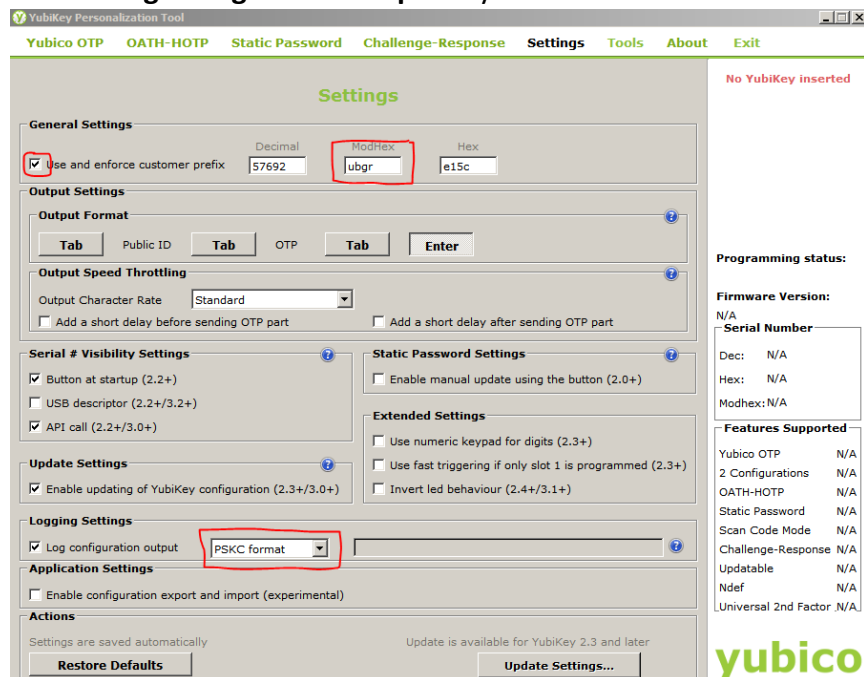
Tento návod opisuje, ako naprogramovať kľúče Yubikey v režime OATH HOTP. Výsledné OTP - jednorazové heslo - bude mať 18 znakov namiesto predvolených 44 znakov.

2. PREDPOKLADY

- Máme všetky Yubikey, ktoré chceme naprogramovať
- Stiahnite si a nainštalujte do počítača nástroj Yubico Personalization Tool (k dispozícii tu)
- Ak potrebujete ďalšie kľúče Yubikey, môžete si ich kúpiť tu

3. NAPROGRAMOVANIE KLÚČOV YUBIKEY

1. Otvorte **Yubico Personalization Tool**
2. Vyberte položku ponuky "**Settings**".
 - a. Kliknite na "**Use and enforce customer prefix**" a do poľa ModHex zadajte "**ubgr**".
 - b. V časti "**Log configuration output**" vyberte možnosť "**PSKC**".



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

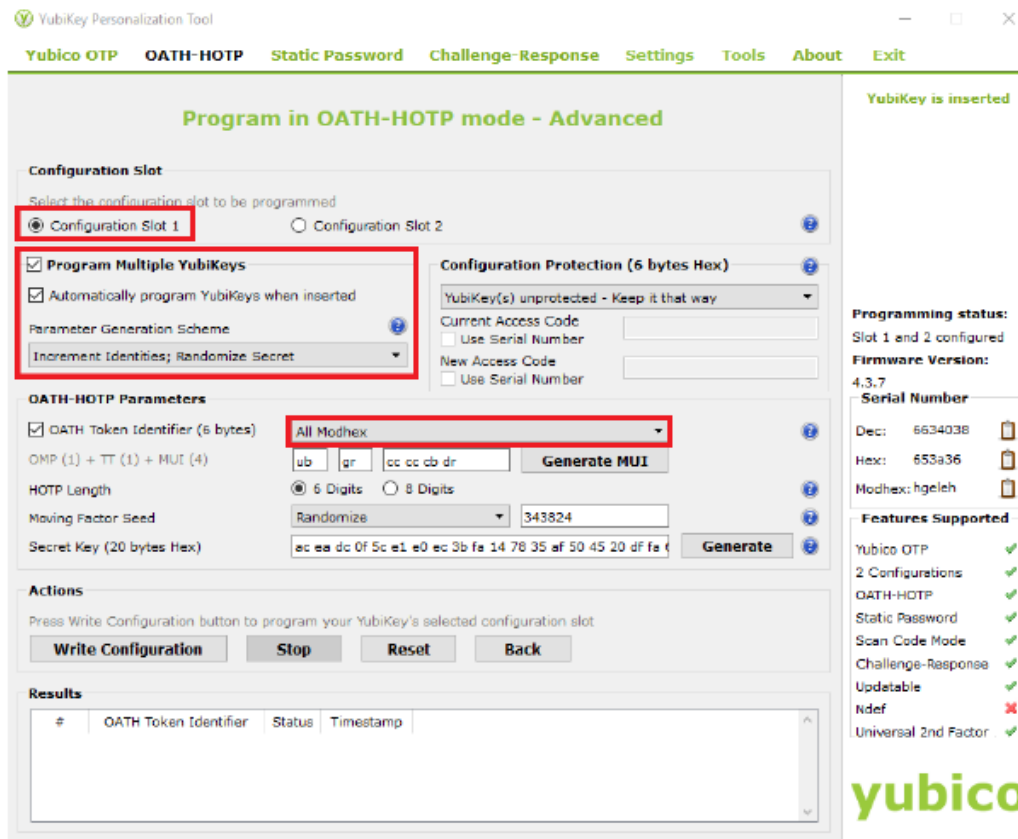
Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

yubico

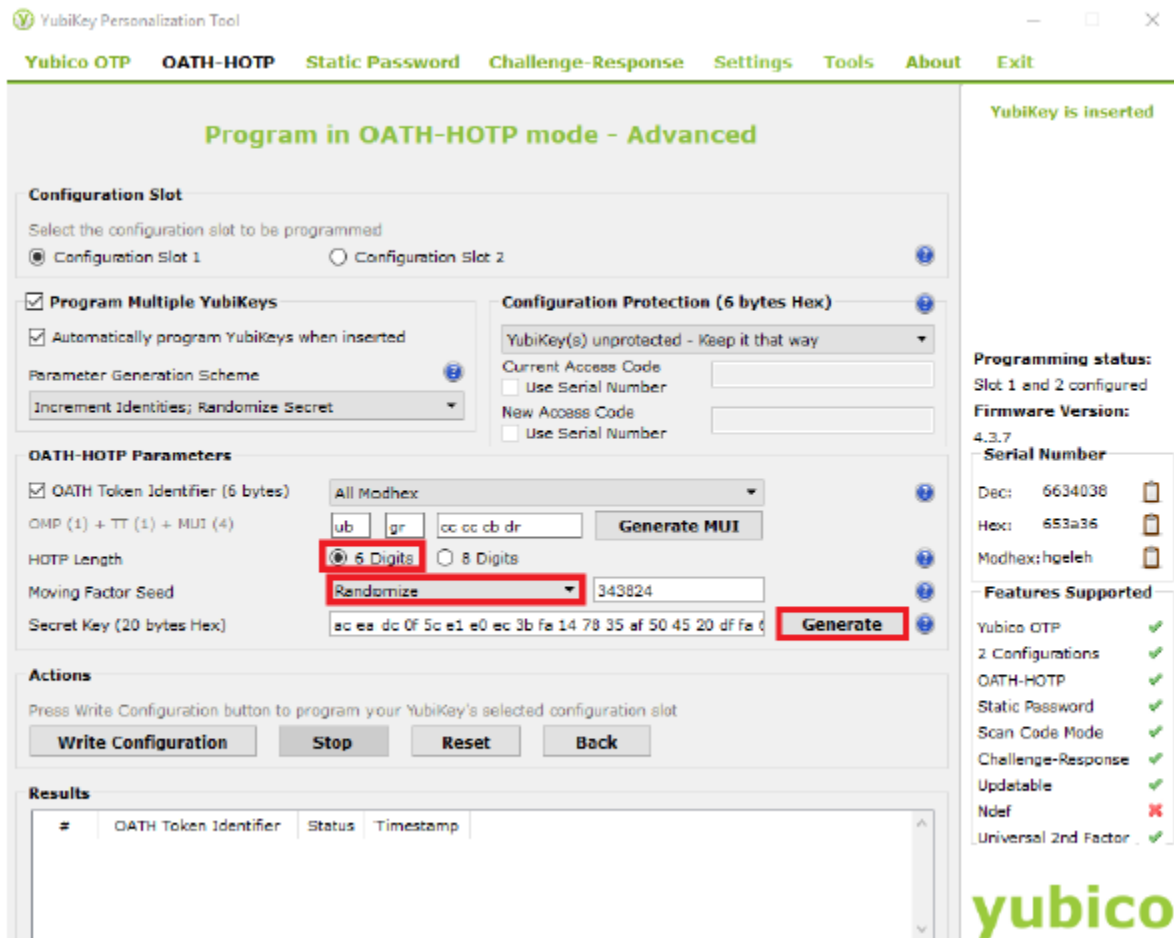
3. Vyberte položku **"OATH-HOTP"** a kliknite na **"Advanced"**.



4. Zobrazí sa nasledujúca obrazovka, pozri nižšie:
 - a. Vyberte položku **"Configuration Slot 1"**.
 - b. Vyberte položku **"Program Multiple Yubikeys"**
 - c. Vyberte možnosť **"Select Automatically program YubiKeys when inserted"**.
 - d. V časti **"Under Parameter Generation Scheme"** vyberte možnosť **"Increment Identities; Randomize Secret"**.
 - e. V časti OATH-HOTP Parameters vyberte položku **"All Modhex"**



- Nastavte dĺžku HOTP na "6 digits" a "Moving Factor Seed" na "Randomize" a kliknite na tlačidlo "Generate" alebo na vygenerovanie predpokladaného tajného kľúča.



YubiKey Personalization Tool

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

Program in OATH-HOTP mode - Advanced

YubiKey is inserted

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:
 Use Serial Number
 New Access Code:

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

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

- Vložte prvý Yubikey a kliknite na tlačidlo "Write Configuration". Výstupný súbor pomenujte a uložte. (Poznámka: uistite sa, že výstupný súbor neobsahuje žiadne znaky medzery.) Tento súbor bude obsahovať bezpečnostné údaje naprogramovaných kľúčov Yubikey. Uchovávajte ho na bezpečnom mieste, kým nebude vložený do systému GreenRADIUS. Potom ho po nahratí odstráňte.
- Už vložený Yubikey sa naprogramuje a v tomto prípade sa zobrazí správa o jeho úspešnosti. Odstráňte zariadenie Yubikey.
- Bez toho, aby ste ukončili aplikáciu, vložte ďalší Yubikey. Počkajte, kým program naprogramuje vložený nástroj Yubikey (ak sa to podarí, zobrazí sa správa), a potom ho vyberte. Pokračujte v tomto postupe so zvyšnými kľúčmi Yubikey.
- Po naprogramovaní všetkých zariadení Yubikeys kliknite na tlačidlo "Stop" a zatvorte aplikáciu.

4. IMPORTOVANIE NOVÉHO SÚBORU SECRET DO PROGRAMU GREENRADIUS

- Otvorte nové okno v prehliadači a prejdite na webovú stránku správy GreenRADIUS.
- Uistite sa, že validačný server je nastavený na "Local Validation Server on GreenRADIUS". Túto možnosť možno nastaviť na karte "Global Configuration" v časti "Validation Server".

3. Taktiež v časti "**Global Configuration**" na karte "General settings" nastavte "**YubiKey (OATH-HOTP Mode) Configuration – OTP Length**" na hodnotu 6 a uložte pomocou "Save".
4. Prejdite na položku "**Import Secrets**".
5. Vyberte položku "**Import OATH Tokens (PSKC Container)**" a kliknite na "**Browse...**".
6. Vyberte súbor vytvorený počas programovania.
7. Kliknite na tlačidlo "**Upload**". Neopúšťajte webovú lokalitu. Počkajte na správu o úspechu.
8. Po úspešnom odoslaní sa vám na karte "List Tokens" zobrazia novoimportované tokeny.