

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 lérejövő 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.

😯 YubiKey Personalization Tool						<u>- 🗆 ×</u>
Yubico OTP OATH-HOTP Static Password	l Challenge-Response	Settings	Tools	About	Exit	
General Settings General Settings Decimal Image: State of the stat	ModHex Hex				No YubiKey inse	erted
Output Settings						
Output Format Tab Public ID Tab OTP	Tab Enter			•	Programming sta	tus:
Output Speed Throttling				0		
Output Character Rate Standard	-				Firmware Version	n:
Add a short delay before sending OTP part	Add a short delay after	sending OTP	bart		N/A	
Serial # Visibility Settings	Static Password Setting	15			Dec: N/A	
Button at startup (2.2+)	Enable manual update	using the butto	un (2.0+)		Hex: N/A	
\Box USB descriptor (2.2±/3.2±)					Modbey: N/A	
	Extended Settings					
J♥ AP1 Call (2.2+/3.0+)	Use numeric keypad fo	r digits (2.3+)			Features Suppo	rtea –
Update Settings	Use fast triggering if or	ly slot 1 is pro	grammed (2.3+)	Yubico OTP	N/A
Enable updating of YubiKey configuration (2.3+/3.0+)	Invert led behaviour (2	4+/31+)	-		2 Configurations	N/A
ji Endole apadning of rabiticly configuration (Elerrybior)		,			Static Password	N/A
Logging Settings					Scan Code Mode	N/A
Log configuration output PSKC format				0	Challenge-Respons	se N/A
Application Settings					Updatable	N/A
Enable configuration export and import (experimenta)				Ndef	N/A
Actions					Universal 2nd Facto	or _N/A_
Settings are saved automatically	Undate is available f	or YubiKey 2.3	and later			
Restore Defaults		adata Catting			vubid	
		Juare Setting	5		,	



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

YubiKey Perso Yubico OTP	nalization Tool	Static Password	Challenge-Response	Settings	Tools	About	Exit	П	×
Program in OATH-HOTP mode						YubiKey is inserte			
Quick Quickly progr	am a YubiKey in OA	TH-HOTP mode						•	
Advance Allows you to	ed	re YubiKeys in OATH-HO	TP mode with greater control	over the confid	uration value	es Pi	rogramm	ing stat	tus:
						SI	ot 1 and 2	configu /ersion	ired I:
						2.	4.0 Serial Nur	nber	

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

🛞 YubiKey Persona	alization Tool						_	- ×
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	About	Exit	
	Progra	m in OATH-HO	OTP mode - Adva	nced			YubiKey is	s inserted
Configuration 9	Slot							
Select the config Configuration	uration slot to be p Slot 1	rogrammed O Configuration S	lot 2					
🗹 Program Mu	ltiple YubiKeys –		Configuration Protection	on (6 bytes H	lex)	0		
Automatically Parameter Gener Increment Ident	program YubiKaya ration Scheme tities; Randomize S	s when inserted @ secret •	YubiKey(s) unprotected - Current Access Code Use Serial Number New Access Code Use Serial Number	Keep it that w	αγ	•	Programmir Slot 1 and 2 d Firmware V 4.3.7	ng status: configured ersion:
OATH-HOTP Pa	rameters			_			Serial Num	iber
OMP (1) + TT (1)	toentifier (6 bytes)	All Modhex	Conorate	T MILT		e e	Dec: 653	*038 🛄 336 🕅
HOTP Length	,	6 Digits 0 8	Digits	1101			Modhex: hge	leh 🗍
Moving Factor Se	ed	Randomize	▼ 343824			0	Features S	upported
Secret Key (20 b	ytes Hex)	ac ea do Of 5c e1 e	e ec 3b fa 14 78 35 af 50 45	20 df fa (Generate	0	Yubico OTP	
Actions Press Write Conf	figuration button to	program your YubiKey's	a selected configuration slot				2 Configurati OATH-HOTP Static Passwo Scan Code M	ons 🖌
write com	igurativii	Stop Res					Challenge-Re	ssponse 🖌
Results # OATH	H Token Identifier	Status Timestamp				^	Updatable Ndef Universal 2nd	d Factor . 🗸
						~	yub	oico



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

Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools A	lbout Exi	t		
Program in OATH-HOTP mode - Advanced							YubiKey is inserted		
Configuration	Slot								
Select the confi	guration slot to be p	programmed							
Configuratio	n Slot 1	Configuration SI	at 2			0			
🗹 Program Mi	ultiple YubiKeys		Configuration Protection	on (6 bytes H	ex)				
Automatically program YubiKeys when inserted			YubiKey(s) unprotected - Keep it that way			•			
Parameter Generation Scheme (3)			Current Access Code	Current Access Code			amming stat	tus:	
Use Serial Number				Slot 1 a	and 2 configur	red -			
OATH-HOTP P	arameters		Use Serial Number			4.3.7 Seria	I Number		
OATH Token	Identifier (6 bytes)	All Modhex		•		Dec:	6634038	ſ	
OMP (1) + TT (1	L) + MUI (4)	ub ar ac ac	cb dr Generate	MUI		Hext	653a36	ſ	
HOTP Length		6 Digits 0 8	Digits			Modhe	x:hoeleh	ĩ	
Moving Factor S	eed	Randomize	343824			- Feat	ures Support	ter	
Secret Vev (20	huter Hex1	ac ee do 05 5c e1 e	0 ec 3b fe 14 78 35 ef 50 45	20.45.5+4	Cenerate		oto		
Secret Key (20	bytes next		0 80 30 18 14 70 35 81 50 45		dellerate	2 Conf	inurations		
Actions						OATH-	нотр		
Press Write Con	figuration button to	program vour YubiKev's	selected configuration slot			Static	Password		
Write Con	figuration	Stop Res	at Back			Scan C	Code Mode		
	garation		buck			Challer	nge-Response		
Results						Updata	sble		
a CATU Talaa Maatifaa Chatua Timastama						Ndef			
# OAT	H Token Identifier	Status Timestamp				Univers	sal 2nd Factor	٢.	
						VI	ubic	-	

- 6. Helyezzük be az első Yubikey és kattintsunk a "Write Configuration" gombra. Nevezzük el a kimeneti fájlt és mentsük 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.
- 7. A már behelyezett Yubikey felprogramozásra kerül és ebben az esetben annak sikerességéről szóló üzenetet kapunk. Távolítsuk el a Yubikey-t.
- 8. 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.
- 9. Miután minden Yubikey-t felprogramoztunk, kattintsunk a "Stop" gombra és csukjuk be az alkalmazást.

4. AZ ÚJ TITOK FÁJL IMPORTÁLÁSA A GREENRADIUSBA

- 1. Nyissunk meg egy új ablakot a böngészőben és menjünk a GreenRADIUS adminisztrációs weboldalára.
- Győződjünk meg arról, hogy az ellenőrzést végző szerver "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 mentsük 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.