

OTP/HOTP/TOTP

Bevezetés az egyik leggyakoribb 2FA megoldás részleteibe

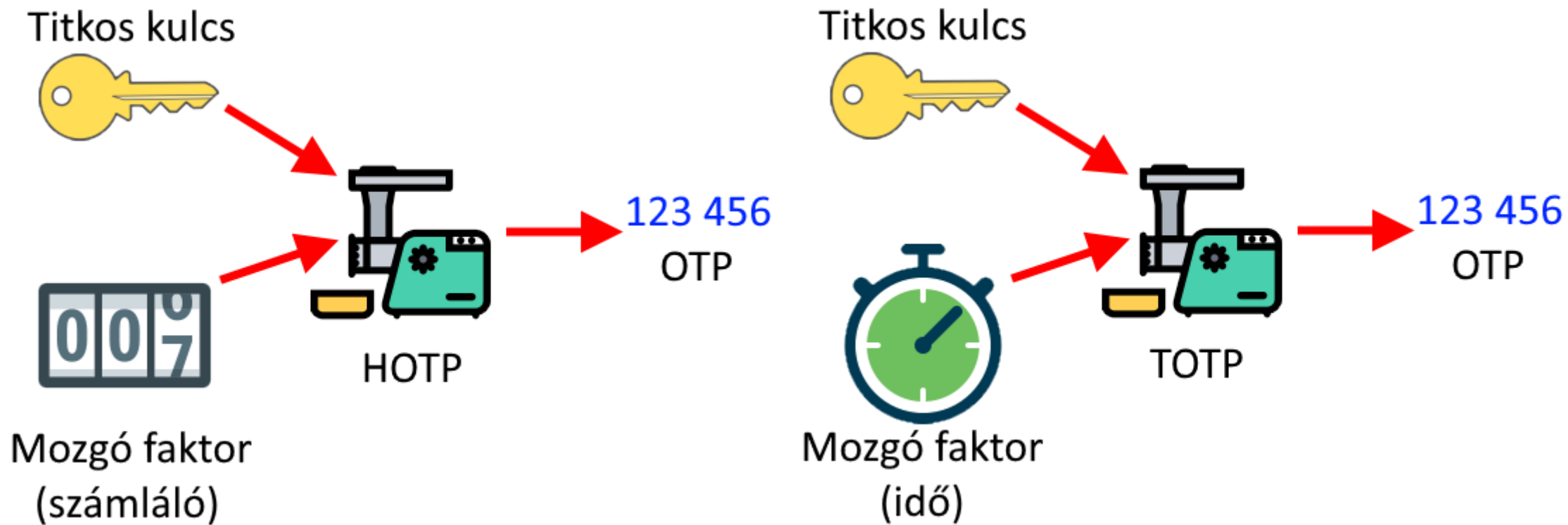
One Time Password típusok bemutatása

- Típusai
 - Idő alapú
 - Lánc alapú
 - Számláló alapú
 - Challenge-response
 - Egyedileg generált
- Megvalósításai
 - SMS/email
 - Hardware token (RSA SecurID, YubiKey)
 - Software token (Authy, Google Authenticator)
 - Nyomtatás

One Time Password szabványok

- Szabványosítás
 - OATH (Open AuTHentication) - <https://openauthentication.org/>
- Szabványok
 - RFC 2289 (OTP)
 - RFC 4226 (HOTP)
 - RFC 6238 (TOTP)

HOTP/TOTP algoritmus



HOTP/TOTP algoritmus

- HOTP
 - $\text{hmacHash} = \text{HMAC-SHA-1}(\text{secretKey}, \text{counter});$
 - $\text{truncatedHash} = \text{hmacHash}$ utolsó 31 bitje
 - $\text{finalOTP} = (\text{truncatedHash} \% (10 \wedge \text{numberOfDigitsRequiredInOTP}));$
- TOTP
 - $\text{hmacHash} = \text{HMAC-SHA-1}(\text{secretKey}, \text{currentUnixTime} / 30);$
 - $\text{truncatedHash} = \text{hmacHash}$ utolsó 31 bitje
 - $\text{finalOTP} = (\text{truncatedHash} \% (10 \wedge \text{numberOfDigitsRequiredInOTP}));$

HOTP-TOTP összehasonlítás

- HOTP-ben előre legenerálható több jelszó
- HOTP-ben széteshet a számláló szinkronja
- HOTP brute-force-olható
- HOTP jelszavaknak nincs lejáratja (létezik köztes megoldás)
- TOTP idő-elcsúszás problémát okozhat (hardware tokenek)

Közös titkos kulcs

- Statikus
 - Előre bedrótzott fix érték
- Dinamikus
 - QR kód
 - Érdemes kiírni is
 - Bizonyos TOTP appokban kézzel is beírható

Set Up a Third Party App to Generate Codes

To get a third party app working, either scan the QR code below or type the secret key into the app.

QR code:



Secret key: **J32F UCFA 4MJ4 QHMJ**

To confirm the third party app is set up correctly, enter the security code that appears on your phone.

Security code:

Cancel

Confirm

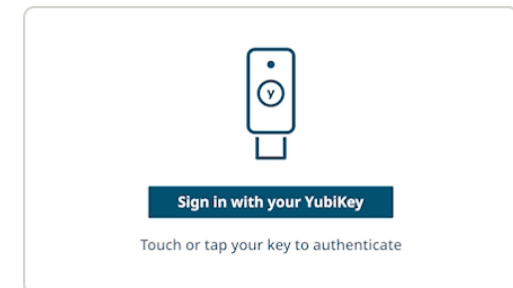
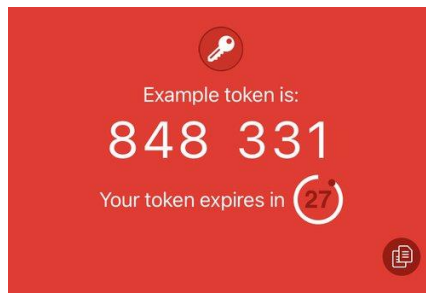
HOTP/TOTP kliensek

- Software

- Authy
- Google Authenticator
- Yubico
- FreeOTP

- Hardware

- Yubikey
- Duo
- Protectimus



TOTP alkalmazás

- Cloud szolgáltatók
 - Google
 - Amazon
 - Microsoft
 - Facebook
 - Cloudflare
- Egyéb protokollok, szoftverek
 - cPanel
 - VPN
 - SSH (Pluggable Auth Module-on keresztül)
- Emailhez nincs jól támogatva
 - Inkább OAuth2

One Time Password biztonság

- Biztonságosabb, ha
 - Van idő szinkronizáció/időkorlát
 - Challenge-response algoritmuson alapszik
- Támadási felületek
 - Social engineering
 - Man-in-the-middle
- Backup
 - Ne oda mentjük, ahova a jelszót!
 - Legtöbb autentikátor app nem tud menteni

Köszönjük a figyelmet!



[Attribution-ShareAlike 4.0 International \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)

Ez a Mű a [Creative Commons Nevezd meg! – Így add tovább! 4.0 Nemzetközi Licenc](https://creativecommons.org/licenses/by-sa/4.0/) feltételeinek megfelelően felhasználható.