OTP/HOTP/TOTP

Bevezetés az egyik leggyakoribb 2FA megoldás részleteibe

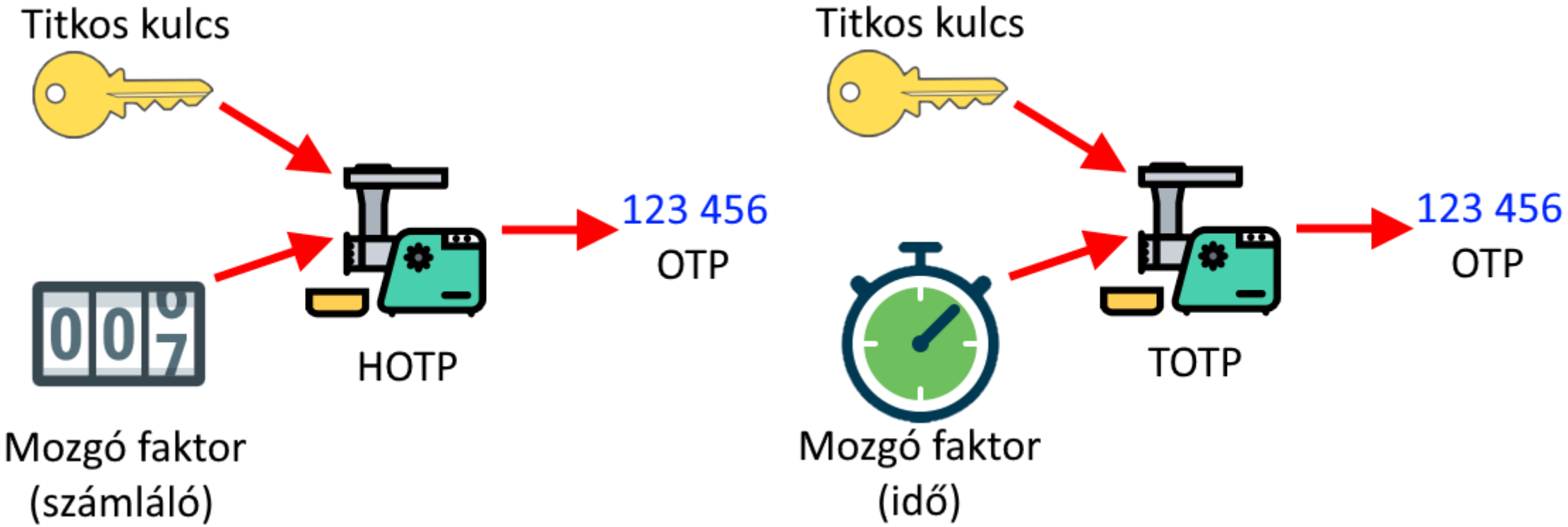
One Time Password típusok bemutatása

- 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

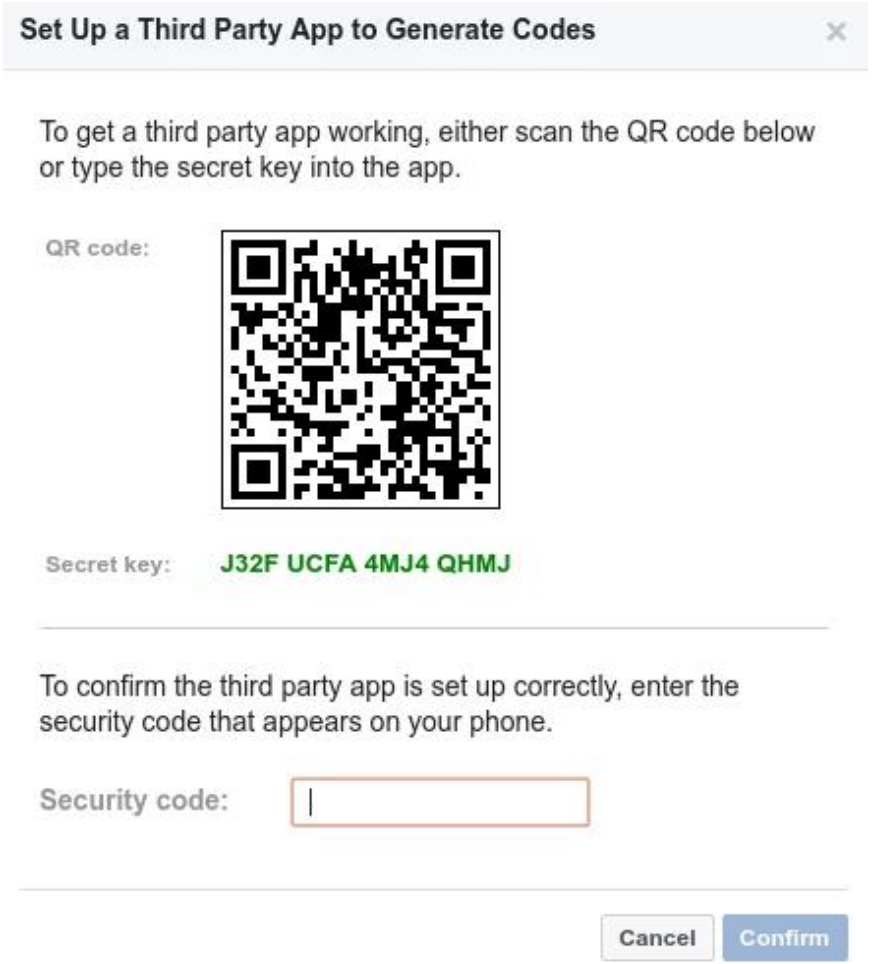
- HOTP
  - hmacHash = HMAC-SHA-1(secretKey, **counter**);
  - truncatedHash = hmacHash utolsó 31 bitje
  - finalOTP = (truncatedHash % (10 ^ numberOfDigitsRequiredInOTP));
- TOTP
  - hmacHash = HMAC-SHA-1(secretKey, **currentUnixTime / 30**);
  - truncatedHash = hmacHash utolsó 31 bitje
  - finalOTP = (truncatedHash % (10 ^ numberOfDigitsRequiredInOTP));

HOTP-TOTP összehasonlítás

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

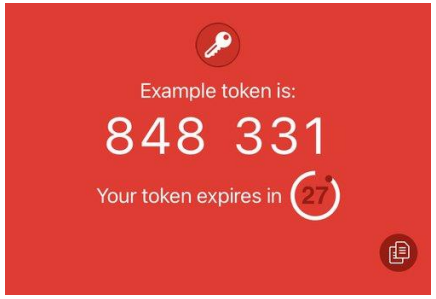
Közös titkos kulcs

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



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 mentsük, ahova a jelszót!
  - Legtöbb authentikátor app nem tud menteni

Köszönjük a figyelmet!