

PKI a mobilon

Public key
Non repudation certificate
Qualified e-Signature
Mobile ID
Private key
Trust Service Provider
Encryption
Time stamp
Authentication
e-Seal
QSCD
Certificate Authority

**eIDAS szerinti bizalmi
szolgáltató**

**Nyilvános kulcsú
Infrastruktúra szakértelem**

ETSI teljes jogú tag

**e-Szignó, PassBy[ME],
Microsigner és eSzemélyi PKI
alapú biztonsági technológia**





Publikus kulcsú infrastruktúra

- Régi barát
- Hasznos barát
- Igazi „egyéniiség”

Azonosítás

Szerver
SSL/TLS

Kliens - Szerver
VPN



Elektronikus aláírás

- Fokozott biztonságú (írásba foglalás)
- Minősített (teljes bizonyító erejű magánokirat)
- Minősített tanúsítványon alapuló fokozott biztonságú (teljes bizonyító erejű magánokirat)

Azonosítás

Kulcsgenerálás/tárolás

Ügyleti érték

Felelősségvállalás



Rabláncok

- Smart Card
- Token
- Tanúsítvány és kulcstárak

A jelszót könnyebb megjegyezni, mint egy 2048 bites RSA kulcsot

Mobil PKI kihívások

- Kulcsgenerálás + tárolás
- Tanúsítvány kibocsátás
- Kulcshasználat
- Kommunikáció

Kulcsgenerálás + tárolás

- Generálás
 - Rendszerszolgáltatások
 - Szoftveres libek vs. jó véletlen
- Tárolás
 - Keychain
 - Android System Keystore
 - PKCS12
 - Passphrase/PIN/Biometria

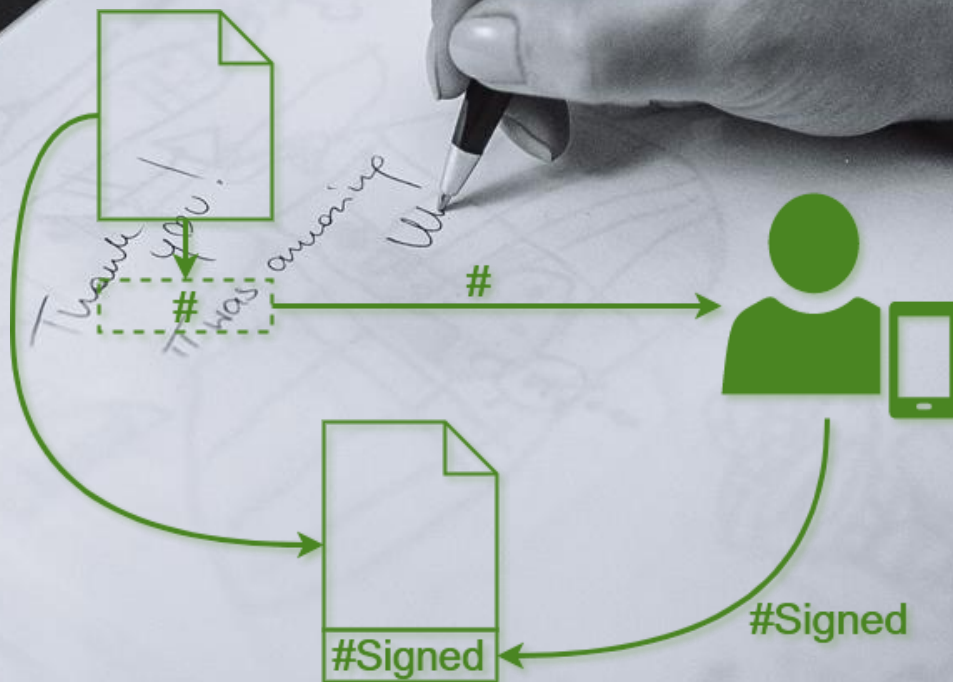
Simple Certificate Enrollment Protocol (SCEP)

- Hitelesítés Szolgáltató közreműködésével
- HTTPS



Kulcshasználat

- PKCS7
- „Kétmenetes” aláírás



Kapcsolat

- HTTPS
- Kliens autentikáció
- Certificate pinning
- OCSP stapling





MICROSEC

A photograph of two men in dark suits and white shirts sitting at a table in a conference setting. The man on the left is seen from the side, looking towards the man on the right. The man on the right is looking back at him. In the background, other people and conference equipment are visible. A yellow vertical bar is on the right edge of the image.

Azt amikor az a bigyó....
Na azt elismétnéd?

Ahhoz nekem is
kell egy sör.