Securing the user experience, with a Smartphone App Authenticator (SAA)

markku.mehtala@meontrust.com – April 2017
Why Smartphone App Authenticator (SAA)?

- Fulfills user expectations of UI and biometrics
- SIM cards are going virtual
- SAA enables dynamic authentication policies
  supporting LoA1 - LoA4
- SAA still enables digital signatures and strong security
Software smartcard in Your app
Dynamic authentication with a simple tap, PIN, fingerprint or face recognition based on Service Provider policies
Strong authentication on any channel

Identity Gateway

Auth API

MePIN server

PKI

Access anywhere

Authenticate and authorize with a digital signature
me pin supports multi-MNO deployments

- ID Gateway MNO1
- ID Gateway MNO2
- ID Gateway MNO3
- ID Gateway MNO4

Country specific Mobile Connect SAA Service

Consumers

Shared self branding MC SAA

MNO App

SAA library

Optional integration into existing self service apps
Flexible deployment, from cloud to on-premise

Client
- Customer's mobile app
  - MePIN library
  - or
  - Customer branded ID app
    - MePIN SDK
  - or
  - Fully hosted

Server
- On-premise
- or
- Mixed (hosted PKI)
- or
- Fully hosted
Active Transaction & Authentication Core (ATAC)

- **Customer App UI**
- **MePIN core library**
- **Mutual authentication and trust**
  - Device fingerprint
  - PKI authentication
  - Device integrity check
- **MePIN server**
- **PKI**
- **Protection against malware & attacks**
  - OS / platform security
  - PIN/FP/Face verification
  - Local data encryption
  - Device - data binding
  - Jailbreak/root detection
  - Whitebox / HW crypto (FIPS certified)
  - Code obfuscation / tamper detection
  - (Opt) Mobile network binding
  - (Opt) SIM card binding
  - (Opt) Trusted Execution Env integration
- **Device & transaction verification**
  - Device revocation check
  - Transaction integrity check
  - Digital signature verification
  - Collecting additional data for 3rd party fraud detection tools
- **Man-in-the-middle protection**
  - TLS binding
  - Encrypted communication
  - Mutual authentication and trust
  - Device fingerprint
  - PKI authentication
  - Device integrity check
  - Man-in-the-middle protection

Complete future proof authentication platform

Mobile PKI + biometrics
FIDO U2F/UAF
Mobile & HW TOTP
SMS OTP
Paper OTP

High security + high usability
Single unified API
Legacy users + fallback options
... because passwords are evil.