Using Android security for governmental PKI: Opportunities and challenges

Android Security Symposium 2015

Pekka Laitinen pekka.laitinen@vrk.fi
Population Register Centre

Outline

- Background
- Opportunities
- Challenges
- Questions

Disclaimer

These are just my thoughts and opinions when considering Android and TEE as a solution for governmental PKI for mobile space.

I do not speak for the Finnish government and I am not saying that these things will happen.

Background

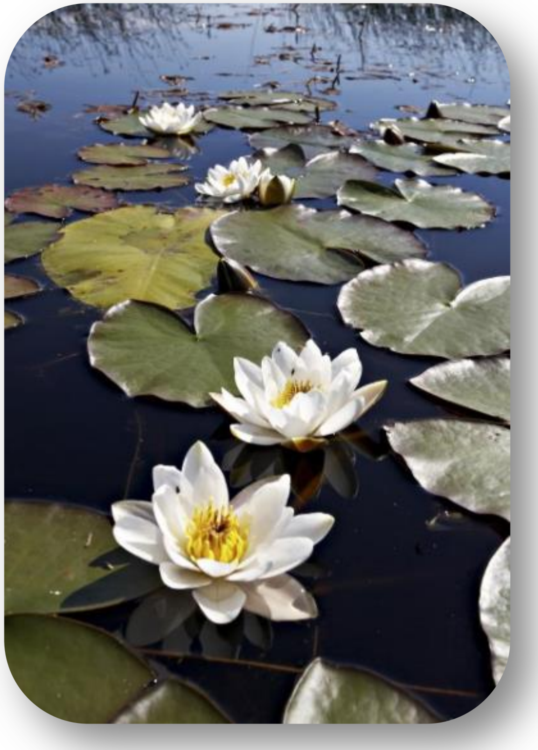
About Population Register Centre

- Two main jobs:
  - maintain population information system
  - governmental PKI (strong identity with smart cards)

- Different kind of smart cards
  - Citizen cards
  - Organizational cards
  - Healthcare cards
  - Passports

Finnish identification scheme

- Bank credentials (one time passwords, key apps)
- Mobile ID (SIM based PKI)
- Citizen cards (smart cards)



Opportunties

Motivation

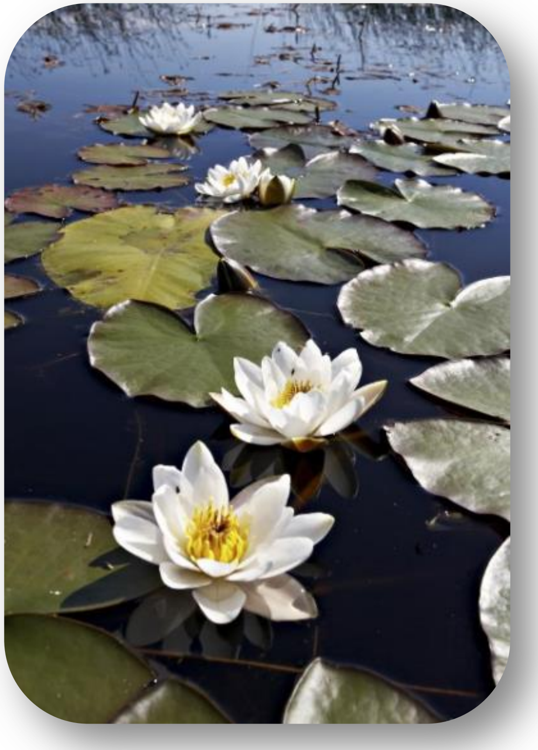
- People use mobile devices more and more
- People want to use services on their mobile device
- Make (strong) authentication easy but secure enough

Alternatives for key protection

- Secure elements
  - Existing smart cards (possibility, needs card reader)
  - Dual interface smart cards (maybe in future)
  - ASSD (possibility, we can issue these)
  - Embedded SE (need to have agreement with owner)
  - UICC (need to have agreement with owner)
- Hardware
  - TPM (not available in mobile devices)
  - TEE (possibility)
- Software
  - Not an option

Mobile OSes and TEEs

- Android
  - TEE based KeyChain
  - EID Trusted Application (TA) on TEE
- iOS
  - Memory encrypted with dedicated AES-chip
  - No TEE (?)
- Windows Phone
  - Virtual smart card (based on TEE via virtualized TPM)
  - ObC TEE (legacy from Nokia times)



Challenges

Requirements

- Platform is trusted
- Private key is protected by TEE
- Private key usage is access controlled by TEE
- Remote attestation key pair (proof-of-key-origin), i.e., Attest that private key is protected by a TEE
- Private key can be used from applications; especially from standard web browser

Trust on platform

- This is the big question: Can Android be trusted?
- Trust needed on hardware, TEE, and EID TA
- Trust on Android as operating system is not needed
- We cannot do what corporations do
  - Device management, custom firmware
- Certification of TEE would be appreciated
- Establish new CA for mobile devices
  - Service providers can decide whether to trust this

Android KeyChain

- KeyChain keys can be used by Android applications
- KeyChain can use hardware protected keystore
  - Application can ask if keystore is protected by hardware but this results to boolean value
  - So, as CA provider we really cannot be sure of this
  - Remote attestation would be nice
- Importing key pair to KeyChain
  - Key pair must be generated in software: not good
- Key usage access control implemented in software
  - Access control based on device lock
  - We need it to be done in hardware

EID Trusted Application in TEE

- Implement EID TA with
  - Key pair generation
  - Usage of key pair is access controlled with passphrase/PIN
  - Private key operations (sign, decipher)
  - Remote attestation with “EID TA key” (generated and certified during EID TA setup)
- Provides own JCE APIs
  - KeyStore, Signature, Cipher, KeyPairGenerator, etc.
  - Implemented as Service, available via Binder
  - Uses own user interfaces (e.g., for PIN query)
- Not part of Android security:
  - Applications need to be aware of JCE APIs

Getting certificate

- Registration of end user; two ways to do it
  - Visit registration office in person
  - Self-service: Use existing credential to do online registration
- Bind registration with certificate enrollment, e.g.,
  - Register on PC with existing credential
  - Use QR code to transfer the session to mobile device
  - Enroll certificate on mobile device with CA
    - Use remote attestation
- Have dedicated application to assist end user to get certificate easily and securely

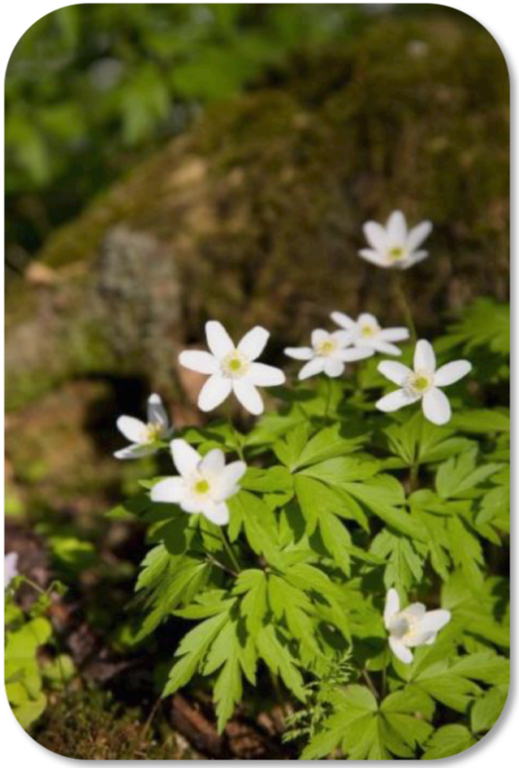
Usage of private key

- Applications need to be aware of JCE APIs
  - Integration and recompilation needed

- Web browser can use ”Signature Creation Service”
  - Produces digital signatures
  - Platform and browser neutral
  - Based on Cross-Origin Resource Sharing (CORS)
  - No need for browser extensions or plugins
  - More information: http://developer.fineid.fi/scs/

Wish list

- Android OS & TEE:
  - certification
- Android OS:
  - ability to extend Android security with new security providers
- KeyChain:
  - remote attestation
  - key pair generation in hardware
  - hardware based access control



Questions