Mobile PKI

- Demo
- Overview / Terminology
- Use cases
- Trust
- Costs
- Feedback
Table 2: Signature Fingerprint Request
Overview - DigiNotar
Overview - Methics
Use cases

- Authentication (Fingerprint signing)
  - Login to (web) applications
  - Certificate requests (replaces USB token)
  - VPN access
  - ... ?
- Digital Signatures (WYSIWHYS)
  - Sign emails
  - Electronic payment
  - ... ?
Enrollment

- Key generation
  - On SIM (by user?)
  - By CA or RA?
- Certificate creation
  - CSR constructed based on public key and proof-of-possession by SIM (link to individual?)
  - CSR then signed by CA
  - Certificate accessible from “Home MSSP”
Trust from user POV

- Application Provider (AP)
- SIM (and phone?)
- Mobile Operator
  - Provides SIM
  - OTA/WIG server (for naive users)
- CA/RA
Feedback

• Good idea?
  • Complexity?
  • Usability?
• Other use cases?