



Ministry
of Digital Affairs



Expert Group Meeting
on
THE BEST PRACTICES IN
IMPLEMENTATION OF MOBILE
IDENTIFICATION (mID)

18-19 October 2016

Warsaw, Poland

Ministry of Digital Affairs



Ministry
of Digital Affairs



Session 1: Overview about Estonian eID

- Population: 1,3 million
- 2000 - Digital Signature Act
- 2002 - Introduction of national electronic ID-card
- 2007 - Introduction of Mobile-ID
- 3 different state granted eID-s
 - 1 277 212 active ID-cards
 - more than 500 000 active users
 - ID card is mandatory document
 - 100 000 Mobile ID users
 - Digi-ID, chip card only for digital usage
- Only ID-card is physical identity document, Mobile-ID is only for digital usage



Ministry
of Digital Affairs



Session 1: Overview about Estonian eID-s

- All eID-s have:
 - Certificate for authentication
 - Certificate for digital signing
- Ca 15M transactions per month, incl:
 - 6M digital signing transactions
 - 9M authentications
 - Ca 3M of them are Mobile-ID transactions
- eID use cases
 - Banking (login and confirm transactions, in EE more than 70% of transactions done in financial sector)
 - Communicating with the government
 - Health sector (access medical data and book doctor's appointment over the Internet, e-prescriptions)
 - Different eServices (self-service portals, eShops)
 - Sign documents digitally, legally binding signature



Ministry
of Digital Affairs



Session 1: Overview about Estonian eID-s

- 99% Of state services are online (www.eesti.ee – portal for citizens and enterprises). <https://www.eesti.ee/eng/services>
- I-voting - 30% vote online
- Banking is online 99.8%
- E-taxes 98% online
- E-prescriptions 99%
- Easy business in 18 minutes
- State owned desktop software for digital signing (digidoc3)



Ministry
of Digital Affairs



Session 2: Business Models

- Involved parties:
 - MNO
 - Mobile-ID service provider
 - Certification Authority (CA)
 - State
 - End-users
 - eService providers
- CA acts as Mobile-ID service provider also
- Mobile-ID platform is provided by private sector
- CA service (certificates) is ordered by state



Session 2: Business Models

- Fees:
 - End-user has to pay state fee to get Mobile-ID
 - End-user has to pay monthly fee to MNO having a Mobile-ID
 - MNO pays to Mobile-ID service provider for using Mobile-ID platform
 - CA gets money for selling certificates (covered by the state)
 - CA asks transaction based fees from eService providers
 - Authentication
 - Digital signing
 - No transaction based fees for end-users. Usage of Mobile-ID is free of charge for private usage



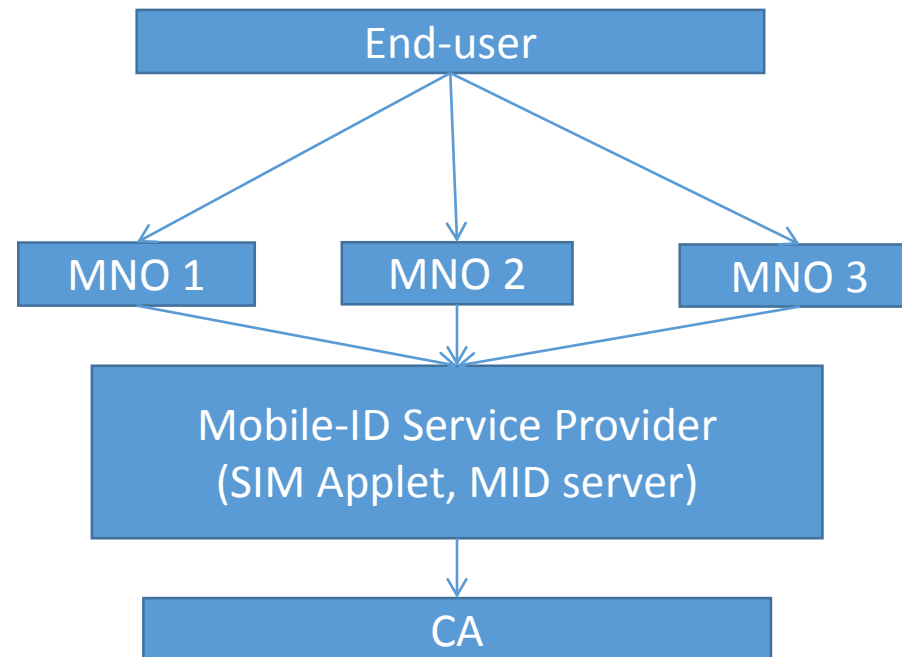
Session 3: IT and Technical Architecture: Solutions, Services and Advantages

- 2007 – 2014 all MNO's has their own technology
 - Different SIM applet (different user experience)
 - All MNO's has their own costs
- Since 2014 there are centralized Mobile-ID service provider
 - Same SIM applet (same user experience)
 - Shared costs for infrastructure
- SIM based PKI solution
 - No biometrics used
 - In house development + part from the market
 - All actions are logged by CA
 - Users can see all their transactions



Session 3: IT and Technical Architecture: Solutions, Services and Advantages

- Enrollment process





Session 4: Security and Privacy:

- It is PKI based solution
- Secure keys are stored on the SIM card
 - The Mobile ID customers' private key is under her/his control
- Messages to and from SIM are encrypted and decrypted only for the mobile user to see
- PKI certificates (RSA2k, ECC) are used
- Using at least Level EAL 4+ SIM cards
- QSCD solution
- CA keeps secure logs about the PKI side



Session 4: Security and Privacy:

- Same level of e-identity as ID-card
- Issued on the basis of the identity document
 - Face-to-face verification by MNO
 - Digitally signed application (with ID card)
- Works as Single-Sign-On solution
- Strong authentication and legally binding digital signature
 - PIN1 - personal identification
 - PIN2 - digital signature
 - PUK code - unblocking Mobile ID PIN
- Most critical part is enrollment process!
- It must be trusted by the all parties on the ecosystem



Session 5: mID use cases and processes: Is it a real usage?

- Mobile-ID is only for digital usage
- Available to all citizens 16+
- Ca 3M Mobile-ID transactions per month
- Banking (login and confirm transactions, in EE more than 70% of transactions done in financial sector)
- Most of service providers who supports ID-cards supports Mobile-ID also
- Sign documents digitally, legally binding signature



Session 5: mID use cases and processes: Is it a real usage?

- Two step registration process:
 - Get Mobil-ID SIM card from MNO (face-to-face verification)
 - Login to police webpage with ID-card and sign digitally application for Mobile-ID
- For suspension call to the MNO 24/7 support line
- Transactions:
 - Enter your phone number to the eService web page
 - Receive message to the phone
 - Verify security code (same random number)
 - Enter PIN code



Session 6: Aspect of awareness raising and information campaign: Are we well aware of mID?

- We have more than 100 000 Mobile-ID users
 - Mobile-ID users are more active than ID-card users
 - Who have tried once, they become fans of Mobile-ID
 - Mobile-ID is more convenient than ID-card
- Our main concern is that we have more than 500K active ID-card users 😊
- It's not easy to change customers habits



Session 6: Aspect of awareness raising and information campaign: Are we well aware of mID?

- Initiative „Smart Security 2018“
 - To educate people about new devices and new threats
 - Target to have 300K+ Mobil-ID users by 2018
 - Main banks, MNO-s, IT companies and state are involved
- Weaknesses
 - It is SIM based. What's about eSIM?
 - App based solutions?
 - Cloud based solution?
 - eIDAS and authentications/signing levels?