Mobile ID (Mobile PKI)

Yahya Salim Alazri
Director of National Digital Certification Center (NDC)
Information Technology Authority
Sultanate of Oman
Agenda

- Session 1: Challenges and Opportunities
- Session 2: Business Models
- Session 3: IT and Technical Architecture
- Session 4: Security and Privacy
- Session 5: MPKI use cases
- Session 6: Marketing and Awareness
The Challenges
- Face to face identity verification and authenticate
- Physical existence at service providers’ premises to sign documents
- Allocation of additional human resources for 24/7 service to carry out business process

Implementation of e-Oman Strategy 2010
- Readiness Assessment (96 Government Entities)
- 80:20 Plan (20% of critical entities provide 80% of government services)
- Business Process re-engineering
- Transfer Government Services from physical to electronic (Systems and Applications)
- ITA’s Billers (Governance, NDC, ISD, OGN, PKI, and OCERT)
**As Is**

- Manual means of identification and Signature services
- Limited availability of human resources and time constraints
- Electronic transaction are not fully compliant with Oman E-Law/69-2008
- Limited capabilities for verifying and approving e-transactions
- Lack of segregation between personal and corporate liabilities
- Lack of strong mechanisms to protect highly valuable transactions or personal information

---

**Roll out Oman PKI**

- People & Organization
- Policies & Standards
- Processes & procedures
- Tools & Technologies
- Metrics & Measurement

---

**To be**

- Electronic means of Authentication and Signature requirements
- No human intervention and time constraints
- E-transaction are fully compliant with Oman E-Law/69-2008.
- Segregation between personal and corporate liabilities using Oman eID, Mobile PKI, or Secure Tokens
- Strong mechanism to protect digital identities
- Means to protect and avoid disclosure of data to unauthorized parties
- Secure single-sign-on for e-government services
Session 1

History: Oman National PKI Project

- RFP Floating: January 2011
- Bidders Proposals (International 13 Companies)
- Vendor Selection and Contracting: August 2011
- System and Hardware: OpenTrust (PKI+CMS), Valimo and Safenet
- Project Implementation Kick-off: November 2011
- RCA, CAs Key Creation: June 2013
- RAs Setup (ROP, Omantel, Ooredoo): July 2013
- Go Live: 14-July-2013
PKI Objectives

- To Increase the number of Government’s e-services by providing
  - Electronic digital identity and authentication
  - Electronic signature for online transactions with non-repudiation service

- To prevent identity fraud and increase the level of confidence to exchange information over Internet
  - Through the use of public and private cryptographic key pairs

- To leverage Data Protection
  - compliant with e-transaction laws

- To empower the e-Government Transformation by providing
  - Data integrity
  - data confidentiality
  - strong authentication
  - Non-repudiation
Session 2: Business Models

- Oman National PKI Ownership (Public Based)
  - Owned and operated by ITA as NDCC which provides PKI services to organizations and the public

- PKI Services
  - Authentication
  - Electronic Signing
  - Email Signing and Email encryption
  - Server SSL Authentication
  - Client SSL Authentication
  - IPSec/VPN Security
  - Time Stamping
  - OCSP Responder
Session 2: Business Models

- PKI Services Fees
  - NDCC Service Catalogue: Competitive Prices, Subsidized by ITA

- eID exchange
  - Oman IDP
Oman National PKI Hierarchy
Session 3: IT and Technical Architecture

Level 1: Offline
- Root CA

Level 2: Offline
- Government CA
- Commercial CA

Level 3: Online
- Corporate CA
  - eID CA
  - Devices CA
- Devices CA
- Individual CA
- Mobile PKI CA
PKI Electronic Identity Gateway

- Web based application hosted in Oman National PKI Center.

- Advantages to service providers
  - Strong user authentication by a trusted identity provider; ITA
  - Transactions: non-repudiation service (using electronic signature with time stamping)

- Advantages to users
  - Single Sign On -- No need to remember dozen of usernames and passwords
  - No need for client software in user’s computer
  - End-users can access online services in a secure and convenient way
Session 3: IT and Technical Architecture

- Authentication
- E-Signing
- Mobile ID
- ID card
Mobile PKI
Mobile PKI (Mobile eID) is a natural development for eID cards when used for electronic authentication and digital signing - with a simple PIN code and a mobile phone.

Combines end user convenience with superior security enabling strong authentication and legally binding signatures.

Equivalent to a personal handwritten signature.

For **Citizens** and **Residents** (Oman eID Holders).

Can be used by Mobile Operators and Banks for apps/call centers authentication (online login), and documents signing.
Based on a strong two factor mobile authentication

- More secure than other existing technologies for authentication and transaction signing
- Protects SP and their users from phishing and identity theft attacks

PKI-enabled SIM Card includes a dedicated hardware processor optimized for RSA cryptographic operations and key generation

**VMAC applet**: a SIM Mobile Authentication Client which supports onboard key generation and PIN management
Session 4: Security and Privacy

- Security and Privacy (PKI Infrastructure and Secure Network)
- certification body: NDCC
- security requirements
- PKI registration Verification:
  - ID Card (Police Civil Status): Face and Fingerprint
  - Mobile PKI (Telecom Outlet – ID Card) + Online Activation
  - Tokens (RA Operators)
- Users Privacy
Session 5: MPKI use cases

- Real Integrated System: 26 integrated to PKI for 14 entities
  - Invest Easy, Man Power, Ministry of Health, Oman Royal Policy, Public Prosecution, Muscat Municipality, Alrafd Fund ..etc
  - Bank Dhofar

- MPKI implementations: Authentication and e-signing

- MPKI registration: next slide

- MPKI registration: next slide
1. User goes to MNO Counter

2. MNO enters subscriber data with MSISDN number tied to SIM card with ICCID number.

3. MNO register the new SIM card

4. MNO sends the “Subscriber register request to ITA Registration Server.

5. Subscribers' data and card data are saved to ITA VRS db.

6. VRS response status of request to MNO.
Mobile PKI Transaction Flow

1. Signing or authentication process has been started from Service Provider application.
2. Signature request has been sent to ITA-SS.
3. ITA-SS will enquire subscriber certificate details from ITA-RS.
4. ITA-RS will return subscriber certificate details to ITA-SS.
5. ITA-SS will check that returned certificate is valid and will send signature request to ITAMS.
6. ITA-MS will reroute message to mobile phone.
7. User will see signature request and confirm transaction by entering signing or authentication pin.
8. User data is sent back to ITA-MS.
9. ITAMS will reroute data to ITA-SS.
10. ITA-SS will validate signature, check certificate revocation status from CA and send result to Service Provider.
11. User can see certificate details from Service Provider interface.
Mobile Authentication

Introductory screen shown to user

User enters his PIN; a signed response will be sent to ITA Mobile PKI for verification

User receives confirmation and is granted access to the service
E-signing transaction

**Public key, private key solution**
- Private key stored in SIM card
- Private key never leaves SIM card
- On-board key generator

**User PIN**
- Two PIN created by user (sign & Auth)
- Used for authentication and signing
- PIN never leaves SIM card

**Validation**
- Signature validation
- Certificate validation
- Revocation checking (OCSP)

Service Provider

Request (SSL)

Validation status, Signature (SSL)

Mobile PKI solution

Signature request-encrypted

Signature response-encrypted

Request (SSL)
Authentication required

Access to selected service requires authentication. Please proceed by selecting one of the following options:

INVEST EASY SMART LOGIN

Login with e-Government login
To use this method you need civil number and password from ITC self-service machine.

Login with Smart Card/USB token
To use this login method you need ID card and ID card reader.

Login with Mobile ID
To use this login method you need PIN enabled SIM card

Your phone number

Login

Login

Login
## Certificates Issued and Transactions

**Report from: 2013-05-01 to 2016-10-16**

### SIMs report:

<table>
<thead>
<tr>
<th>COUNT</th>
<th>STATUS</th>
<th>OPERATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>5366</td>
<td>Active</td>
<td>Omantel</td>
</tr>
<tr>
<td>3538</td>
<td>Active</td>
<td>ooredoo</td>
</tr>
<tr>
<td>947</td>
<td>Archived</td>
<td>Omantel</td>
</tr>
<tr>
<td>1080</td>
<td>Archived</td>
<td>ooredoo</td>
</tr>
<tr>
<td>6732</td>
<td>New</td>
<td>Omantel</td>
</tr>
<tr>
<td>3336</td>
<td>New</td>
<td>ooredoo</td>
</tr>
</tbody>
</table>

### Transactions report:

<table>
<thead>
<tr>
<th>TOTAL</th>
<th>OPERATOR</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>21675</td>
<td>Omantel</td>
<td>ITA_AUTHENTICATION</td>
</tr>
<tr>
<td>12296</td>
<td>ooredoo</td>
<td>ITA_AUTHENTICATION</td>
</tr>
<tr>
<td>80333</td>
<td>ID Card</td>
<td>ITA_AUTHENTICATION</td>
</tr>
</tbody>
</table>
Session 6: Marketing and Awareness

- Business and Development Department
- Concerns: Technical and Legal
- Information and Awareness Division
- Awareness campaigns: services based (with Integrated entities)
Thank You