Sultanate of Oman
Information Technology Authority
National Digital Certification Center

Oman National PKI
AGENDA

PKI Components
Trust Services
PKI Hierarchy
Competent Authority
PKI Hierarchy
Standards
Projects
Statistics
- Oman National PKI is owned and operated by Information Technology Authority (ITA) as the legal competent Authority

- National Digital Certification Center (NDCC)

- Legal Binding: Oman eTransaction Law 69/2008
Provided eServices with PKI

- No human intervention, No time constraints
- Fully compliant with Oman E-Law/69-2008
- Segregation between personal and corporate liabilities
- Strong mechanism to protect digital identities
- Secure Single Sign-On
- Protect Data

PKI Components:
- People & Organization
- Policies & Standards
- Processes & procedures
- Tools & Technologies
- Metrics & Measurement
eTrust Pyramid Components

- Secure eServices & Applications
- Trust Services
- Public Key Infrastructure
- Legal Framework
Trust Services

Oman National PKI

- Electronic Signing
- Authentication
- TSA / OCSP
- Document encryption
- IPSec VPN Security
- SSL certificate

Email Signing and encryption

Email

Email

Email

Email

Email

Email
PKI

- Strong authentication
- Electronic Signature
- Non Repudiation
- Encryption
- Mature and proven technology
- Compliances with electronic Laws
Added Value

1. Protection against Identity Fraud

2. Data Integrity
   - Data Confidentiality
   - Strong Authentication
   - Non Repudiation

3. Trust and Confidence

4. Easing e-services
- **Oman National PKI**
  
  - **ETSI 102 042** Policy requirements for certification authorities **issuing public key certificates**
  
  - **ETSI 101 456** Policy requirements for certification authorities **issuing qualified certificates**
**Digital Signature Format**

- **ETSI EN 319 142-1** PAdES digital signatures

- **ETSI TS 103 172** PAdES Baseline Profile

- **ETSI TS 102 778-1** PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES

- **ETSI TS 102 778-4** PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile
Time Stamp service

- Time Stamp Authority follows policy requirements on the operations and management practices

- ETSI TS 102 023 V1.2.2 Policy requirements for time-stamping authorities
Standards

Signature Validation Service

- ITA operates its signature validation service (SVS) both as a Trusted Third Party (TTP) for its customers
- ETSI TS 119 441 Policy requirements for TSP providing signature validation services
- 2014: Tender was floated
- 2015: Financial crisis
- 2017: Awarded to EY and kicked-off
- 2018: Remediation Phase – New National PKI
- Will be hosted in a Cloud Environment
- Evaluation Phase
- Award: July 2019
- Digital Signing Solution and Remote Signing:
  - ETSI Long-Term Archive Profiles for PADES, XADES, and CADES
Accreditations

20 February 2019

Registration Authorities

- Royal Oman Police
- Omantel
- Ooredoo
- Central Bank
Integrations (1)

20 February 2019

Statistics

ROP NRS
Omantel
Ooredoo
Invest Easy
ROP Customs
Ministry of Health
Ministry of Manpower
Rafd Fund
ITA
Muscat Municipality
OPP
MARA
Mazad
Bank Dhofar
NCSI
MRMWR
Integrations (2)

20 February 2019

Statistics

Civil Pension
MOI
TRA
PASI
PACI
SGT
PAMR
Oman Info
Alduqum
Oman Post
PEIE
ROP Traffic
Central Bank
MECA
MAF
MOJ
Integrations (3)

20 February 2019

Statistics

MCD

MOE

Tender Board

Oman Chamber
Certificates

July 2013 - February 2019

Oman Population
4.5 M

National ID Card
15.7 M

Mobile
110,882
Transactions

July 2013 - February 2019

Statistics

National ID Card
14.2 M

Mobile
1.7 M
An Entity can be accredited as an External RA to manage its own subscribers

More convenient for conducting subscribers identifications

Registration and Validation Teams will be trained by ITA

Entity must be aligned with National PKI policies and accreditation agreement

ITA will conduct auditing activities periodically and according to the auditing report, PMC might renew or suspend the accreditation
Sub-CA accreditation

- An Entity can be accredited as a Sub-CA and build its own technical solution
- Entity must request license according to the licensing processes
- Entity should meet all the policies and the accreditation agreements approved by ITA
- ITA will conduct auditing activities periodically and according to the auditing report,
  PMC might renew or suspend the accreditation
Information Technology Authority (ITA) is based in Knowledge Oasis Muscat (KOM) building 3, Second Floor.

PHONE | (+968) 24166440
OPEN | 7:30 to 14:30

EMAIL
ndccservices@ita.gov.om

SOCIAL MEDIA
eoman_ita
eOman

eoman_ita
eoman.ita