Oman National
PKI and Digital Identity
What is PKI?
PKI Features
Trust Services pyramid Components
Government eServices
PKI Hierarchy
PKI implementations
Who Uses PKI
Statistics
Set of **Roles**, **Policies**, **Procedures** and **Technical Mechanisms** to create, manage, distribute and revoke digital certificates.

Provides security services such as strong authentication, integrity, confidentiality and non-repudiation.
What is PKI?

- PKI is a security architecture that provides an increased level of confidence.
- PKI enables electronic signature for online transactions with non-repudiation.
- PKI leverages Data Protection as it is compliant with e-transaction laws.
What is PKI?

- PKI enables the exchange of information over the Internet through the use of public and private cryptographic key pairs.
- PKI enables online service providers to identify and authenticate their clients electronically.
OBJECTIVES

Protection against Identity Fraud

Data Integrity
Data Confidentiality
Strong Authentication
Non Repudiation

Trust and Confidence

Easing e-services
PKI Features

- Strong authentication
- Electronic Signature
- Non Repudiation
- Encryption
- Mature and proven technology
- Compliances with electronic Laws
Two Factor Authentication

- Strong authentication
- Mature and proven technology
- Electronic Signature
- Encryption
- Non Repudiation
- Compliance with Electronics Laws

PKI Features

Two Factor authentication for Government and Private Portals and mobile apps
PKI Features

- Strong authentication
- Electronic Signature
- Encryption
- Non Repudiation
- Compliances with Electronics Laws
- Mature and proven technology

Electronic Signature
using private keys securing the data integrity
provides a reliable mechanism using PKI digital signature
to avoid unauthorized disclosure of data using public keys
and regulations Leverage Data protection Acts and all around the world

**PKI Features**

- Strong authentication
- Electronic Signature
- Encryption
- Non Repudiation

**Compliances with Electronics Laws**

Mature and proven technology
Mature and proven technology

PKI Features

- Strong authentication
- Encryption
- Electronic Signature
- Non Repudiation
- Compliances with Electronics Laws

Mature and proven technology

adopted for financial, governments, service providers offering highly and valuable services
eTrust Pyramid Components

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

eTrust Pyramid Components

- Policies, Procedures, People, Hardware and Software required for to generate, share and manage digital certificates.

Public Key Infrastructure
Trust Services

- Signature Validation Services
- Time Stamping
- On Line Revocation Services
- Publication of digital certificates and revocation list.
eTrust Pyramid Components

Secure eServices & Applications

E-Services require strong means of authentication, digital signing and data protection in accordance with the country laws and regulations.
ITA efforts for National 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
Implementations

PKI

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

Authentication
AUTHENTICATION

IDP

Mobile PKI

SIGNING

✓ IDP signing
✓ MPKI Signing
✓ Server Signing

Online Certificate Status Protocol

Time Stamping

2

TSA

OCSP
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

<table>
<thead>
<tr>
<th>Civil Pension</th>
<th>Alduqum</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOI</td>
<td>Oman Post</td>
</tr>
<tr>
<td>TRA</td>
<td>PEIE</td>
</tr>
<tr>
<td>PASI</td>
<td>ROP Traffic</td>
</tr>
<tr>
<td>PACI</td>
<td>Central Bank</td>
</tr>
<tr>
<td>SGT</td>
<td>MECA</td>
</tr>
<tr>
<td>PAMR</td>
<td>MAF</td>
</tr>
<tr>
<td>Oman Info</td>
<td>MOJ</td>
</tr>
</tbody>
</table>
Integrations (3)

20 February 2019

- MCD
- MOE
- Tender Board
- Oman Chamber
Certificates

20 February 2019

National ID Card

- AUTH: 15.7 M
- SIGN:

Mobile

- AUTH: 110,882
- SIGN:
Transactions

20 February 2019

Statistics

National ID Card

14.2 M

Mobile

1.7 M
Accreditations

20 February 2019

Royal Oman Police
Omantel
Ooredoo
Central Bank
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.

ADDRESS

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

EMAIL

ndccservices@ita.gov.om

SOCIAL MEDIA

LinkedIn: eoman_ita
Twitter: eoman_ita
Facebook: eoman.ita