Public Key Infrastructure
PKI

National Digital Certification Center
Information Technology Authority
Sultanate of Oman

January 2014
Agenda

- Objectives
- PKI Features
- eTrust Components
- Government eServices
- Oman National PKI Hierarchy
Agenda

- PKI Implementations
- Electronic Identity Gateway
- Mobile PKI
- Signature Verification
- Accreditation Service
Public key infrastructure is a system of policies, procedures, people, hardware, software and services that support the use of public key cryptography to obtain secure communication.

PKI aims to increase the number of e-services of Government and Private entities to empower the e-Government Transformation as PKI provides:

- Electronic transactions protection against identity fraud
- Data integrity, data confidentiality, strong authentication, and non-repudiation
- Trust, confidence and easiness to use online services for citizens and residents
PKI enables the online service providers to identify and authenticate their clients electronically and enables electronic signature for online transactions with non-repudiation service.

PKI is security architecture provides an increased level of confidence to exchange information over Internet through the use of public and private cryptographic key pairs.

PKI leverage Data Protection as it is compliant with e-transaction laws.
PKI enables the online service providers to identify and authenticate their clients electronically and enables electronic signature for online transactions with non-repudiation service.

PKI is security architecture provides an increased level of confidence to exchange information over Internet through the use of public and private cryptographic key pairs.

PKI leverage Data Protection as it is compliant with e-transaction laws.
Enables strong authentication for the participants requesting electronic services from E-Government agencies.

1. Digital signing electronic form using private keys and protecting the integrity of the data.

2. Avoid unauthorized disclosure of personal data using public keys for encryption.

3. Provide a reliable mechanism to support non-repudiation services through the utilization of digital signature services.

4. Leverage Data protection Acts and compliances with vast government Electronics Laws and regulations all around the world.

5. Mature and proven technology adopted for financial, governments, service providers offering highly and valuable services.

6. January 2014
eTrust Pyramid Components

Legal Framework

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

Trust Services
Signature Validation Services, Time Stamping, On Line Revocation Services, Publication of digital certificates and revocation list.

Secure eServices & Applications
E-Services require strong means of authentication, digital signing and data protection in accordance with the country laws and regulations.
Government eServices

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
PKI Hierarchy

Level 1: Offline
- Root CA
  - Government CA
    - Corporate CA (Email, Encry, Signing, Auth)
    - Devices CA (SSL, IPSec/VPN)
  - Commercial CA
    - eID CA (Auth, Signing)
    - Devices CA (SSL, IPSec/VPN)

Level 2: Offline
- Government CA
  - Corporate CA (Email, Encry, Signing, Auth)
  - Devices CA (SSL, IPSec/VPN)

Level 3: Online
- Government CA
  - Corporate CA (Email, Encry, Signing, Auth)
  - Devices CA (SSL, IPSec/VPN)
- Commercial CA
  - Devices CA (SSL, IPSec/VPN)
  - Individual CA (Encry, Auth, Signing)
  - Mobile PKI CA (Signing, Auth)
PKI Implementations

- Authentication
- Electronic Signing
- Email Signing and Email encryption
- Server SSL Authentication
- Client SSL Authentication
- IPSec VPN Security
- Time Stamping
- OCSP Responder
Oman National PKI
Electronic Identity Gateway
Electronic Identity Gateway is a web based application hosted in Oman National PKI Center.

Organizations are welcome to integrate their online services to get use of it.

Advantages to users

- Single Sign On -- No need to remember dozen of usernames and passwords. A single authentication will provide access to multiple service providers integrated
- No need to install any client software in user’s computer. End-users can access online services in a secure and convenient way.

Advantages to service providers

- Strong user authentication by a trusted identity provider authority; ITA
- Transactions performed with non-repudiation service (using electronic signature with time stamping)
IDP Integration

Service Provider (SP)
- Database
- Web server

SSO, SLO, DSS
Through the browser
Logout

Identity Gateway

- Access to eService
- Communicate with smart card
Authentication with password/smartcard/USB token

- Open SP website
- Redirect the request to IDP
- Signed SAML SSO request
- Redirect the request to SP
- Signed SAML response
- Check SAML response
- session.put(samlCredential)
- Extracting attributes
- SP website page

End user

Smart card

SConnect

Web

Browser

SP

Identity Gateway

January 2014
IDP Integration – Digital Signature Service

End user

Smart card

SConnect

Browser

SP

IDP

Submit secure web form to SP

Redirect the request to IDP

Signed DSS request to IDP

Format data to sign

Check request is from a trusted party and if user is logged in

Digital Signature with smartcard/USB Token

Redirect the request to SP

Signed DSS response with signature to SP

Check DSS response

Log signature result

verifying certificate used to sign belongs to the currently logged in user

Response page
Oman National PKI
Mobile PKI
ITA Mobile PKI is a solution for mobile authentication and signing by a PIN code using a mobile phone.

- Combines superior security and end user convenience.
- Enables strong authentication and legally binding signatures.

October 2013
**Public key, private key solution**
- Private key stored in SIM card
- Private key never leaves SIM card
- Private key is known by nobody
- On-board key generator

**User PIN**
- Personal and created by user itself
- Used for authentication and signing
- PIN never leaves SIM card

**Mobile PKI Architecture**

- Signature request, encrypted
- Service Provider (Bank)
- Validation status, Signature (SSL)
- Request (SSL)
- Mobile PKI solution

**Validation**
- Signature validation
- Certificate validation
- Revocation checking (OCSP)
Mobile PKI Integration

Services require strong authentication can be integrated to ITA Signature Server using the ITA VSS SDK library.

Mobile Activation Client (ITA-VMAC)
- RSA cryptography for digital signatures
- User controlled PIN management

January 2014
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.
Online signature verification
  
  Provides web service interface

If successfully verified (signature is trusted)
  
  Returns proof of verification (PDF document)
  
  No archiving of proof document

Else (verification failure)
  
  Returns error code.

Certify Center uses OCSP and Time Stamping services

Supports:
  
  CMS
    
    ✓ Cryptographic Message Syntax, IETF RFC 5652
    ✓ Derived of PKCS#7 (RSA)
    ✓ Detached or encapsulated

  PDF
    
    ✓ Standard ISO 32000-1
    ✓ ETSI PADES (PDF Advanced Electronic Signature)
    ✓ Embedded signature

January 2014
RA and Sub-CA Accreditation

- **External Registration Authority (RA):**
  - 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
Thank You