PKI Status In Iran
Iran Center for e-Commerce Development
PKI Laws & Regulations in Iran
PKI Laws & Regulations in Iran

- E-commerce Law
- Executive Regulations, Article 32
- Digital Certificate Policy Approved by Policy Council
PKI
Architecture, Usage and Application
Digital Certificate Policy Council

- Governmental Root Certification Authority
- Registration Authority

Iran PKI Policy Authority;
- Approval of Policies, Standards, Procedures;
- Licensing to the CAs;
- Coordinating Authority in Iran PKI.

Certificate Request Management;
- More than 3000 Registration Authorities in Iran PKI.

7 Intermediate CAs in Iran PKI;
- Certificate Issuance and Management for End Entities;

Trusted Point of Iran PKI;
- Governmental Root CA with Permission of the Digital Certificate Policy Council;
- Preparation of Policies, Standards and Procedures;
- Auditing of Intermediate CAs;
- Certificate Issuance and Management of Intermediate CAs;
- Evaluation and accreditation of PKI Related Hardware and Software.

PKI Architecture, Usage and Application

- OGICA
- 2 ICMGCA
- 3 MoPCA
- 4 MOHME CA
- 5 PARSSIGN CA
- 6 RAHABAR TRUST CA
- 7 SMART TRUST CA

Digital Certificate Policy Council

Governmental Root Certification Authority

Governmental General Intermediate CA

Registration Authority

Governmental Intermediate CA

Registration Authority

Private Intermediate CA

Registration Authority

- Certificate Request Management;
- More than 3000 Registration Authorities in Iran PKI.
PKI Architecture, Usage and Application

Digital Signing

- High Assurance Level of Confidentiality Keys
- Medium Assurance Level of Confidentiality Keys
- Basic Assurance Level of Confidentiality Keys
- Rudimentary Assurance Level of Confidentiality Keys

Certification

- Organization Stamp
- Code Signing
- Server (SSL/TLS/DC)

Assurance Level

- Level 1: Bronze
- Level 2: Silver
- Level 3: Gold
- Level 4: Platinum

Electronic Authentication (Login)
PKI Architecture, Usage and Application

Application Areas

- Banking
- Trading
- Procurement
- Stock Market
- Other
PKI Laboratory
- **Cryptographic Modules Laboratory**: for testing and evaluation of **Hardware Security Modules**
  - Smart Card
  - USB Token
  - HSM (Internal/External)
- **CA Management Software Laboratory**: for testing and evaluation of digital certificates **issuing and managing products**
  - CA, RA, OCSP, TSA, ...
- **PKE Application Laboratory**: for testing and evaluation of **PK-enabled applications**
  - Web based Applications
  - Stand alone Applications
- **Cryptographic Algorithm Laboratory**: for testing and evaluation of **Cryptographic Algorithms**
  - Cryptographic Algorithms (Symmetric, Asymmetric, ...)
Iran is very interested to establish a trust relationship to meet the requirements of interoperability and agreed implementation solutions between its CAs and other countries particularly those that are the largest trading partners of Iran.

The validation and acceptance of digital certificates issued by foreign certificate authorities shall be subject to a mutual agreement between Iran's Root CA and the foreign certificate authority with consideration of the reciprocity principle and approval of digital certificate policy council.
Works/Projects
Works/Projects

Issuance of Bank Melli Iran Intermediate CA Certificate

Issuance of qualification certificate for the CAs applicants, audit, and review their technical documentation:

1. PENDAR KOOSHK IMEN
2. RUNC
3. PARS ONLINE TELECOMMUNICATIONS
Works/Projects

- Defining the framework and requirements of the mobile PKI
- Holding consultation meetings with the stakeholders of the mobile PKI services
- Implementing digital signature certificates in mobile platform for using in some financial systems
Works/Projects

- PKI-enabling in the software systems of the SAPCO company with the cooperation of the GICA CA
- PKI-enabling in the software systems of Iran road maintenance and transportation organization with the cooperation of the GICA CA
- PKI-enabling in the software systems of medical council with the cooperation of the MOHME CA
THANK YOU
For Your Attention