PKI Status In Iran

IRAN Center for
eCommerce Development

©Templateswise.com

- PKI Laws & Regulations in Iran
- PKI Architecture, Usage and Application
- PKI Laboratory
- PKI Interoperability
- Future Works

PKI Laws & Regulations in Iran

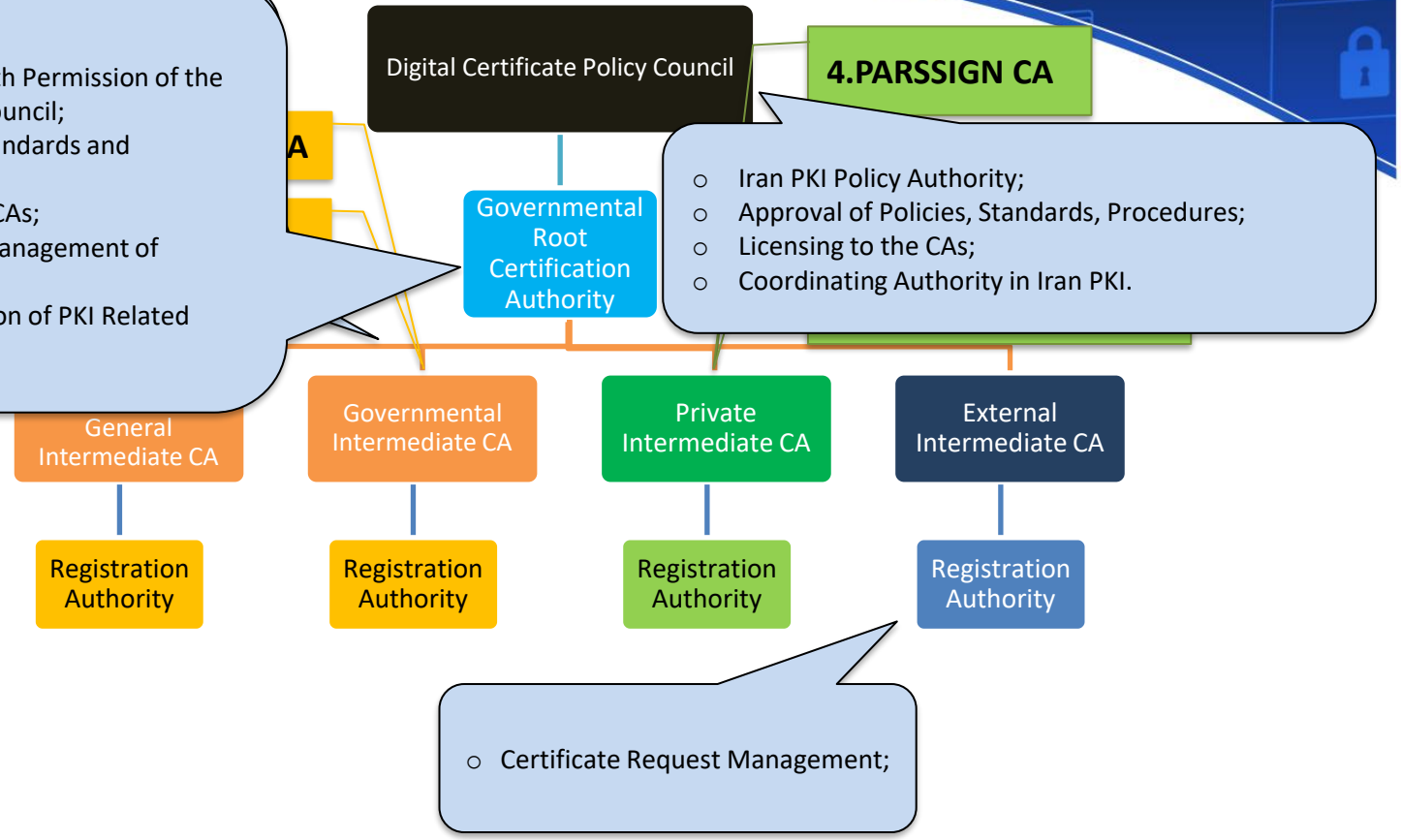
PKI Laws & Regulations in Iran

- E-commerce Law
- Executive Regulations, Article 32
- Digital Certificate Policy Approved by Policy Council

PKI Architecture, Usage and Application

PKI Architecture, Usage and Application

- 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.



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

- Certificate Request Management;

PKI Architecture, Usage and Application

PKI Architecture, Usage and Application

Application Areas

PKI
Laboratory

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 , …)

PKI Interoperability

PKI Interoperability

E-commerce Law

Executive Regulations, Article 32

Article 18

- 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.

Future Works/Projects

Future Works/Projects

Mobile PKI

- Increasing demand for mobile phones and applications
- To build a trust way between users and service providers for using electronic services
- Accessibility of mobile phones in comparison with tokens
- As a developed model of eID cards to facilitate electronic authentication and digital signature with more security consideration

Future Works/Projects

Digital Signature Service

DSS (Digital Signature Services) is an open-source software library for electronic signature creation and validation.

It supports the creation and verification of interoperable and secure electronic signatures.

DSS can be re-used in an IT solution for electronic signatures to ensure that signatures are created and verified in line with legislation and standards.

DSS allows re-use in a variety of different ways: in an applet, in a stand-alone application or in a server application

Future Works/Projects

CA Management

- Non-Face-to-Face Renewal of Digital Certificate
- Issuing 2-year certificates.
- PKI Monitoring System
- New Identity Verification

THANK YOU

For Your Attention