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.

Digital Certificate Policy Council

Governmental Root Certification Authority

4. PARSSIGN CA

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

General Intermediate CA

Governmental Intermediate CA

Private Intermediate CA

External Intermediate CA

Registration Authority

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

Assurance Level

Organization Stamp

Code Signing

Server (SSL/TLS/DC)

High Assurance Level of Confidentiality Keys

Medium Assurance Level of Confidentiality Keys

Basic Assurance Level of Confidentiality Keys

Rudimentary Assurance Level of Confidentiality Keys

Digital Sign (Document Signing)

Certificate Usages

Level 1: Bronze

Level 2: Silver

Level 3: Gold

Level 4: Platinum

Authentication (Login)

Organizational Stamp Code

Signing Server (SSL/TLS/DC)

Authentication (Login)

Digital Sign (Document Signing)

Organization Stamp

Code Signing

Server (SSL/TLS/DC)

High Assurance Level of Confidentiality Keys

Medium Assurance Level of Confidentiality Keys

Basic Assurance Level of Confidentiality Keys

Rudimentary Assurance Level of Confidentiality Keys
PKI Architecture, Usage and Application

Application Areas

- Banking
- Trading
- Procurement
- Stock Market
- Other
PKI Architecture, Usage and Application

Statistics of Issued Certificates

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Issued Certificates</td>
<td>26,218</td>
<td>59,444</td>
<td>161,169</td>
<td>246,251</td>
<td>309,892</td>
<td>363,574</td>
<td>440,188</td>
<td>549,672</td>
</tr>
</tbody>
</table>

Iran population: 82,792,205
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
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.

- 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.
THANK YOU
For Your Attention