PKI Status In Iran

Iran Center for e-Commerce Development

IRAN Center for
eCommerce Development

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

IRAN Center for
eCommerce Development

PKI Laws & Regulations in Iran

IRAN Center for eCommerce Development

PKI Laws & Regulations in Iran

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

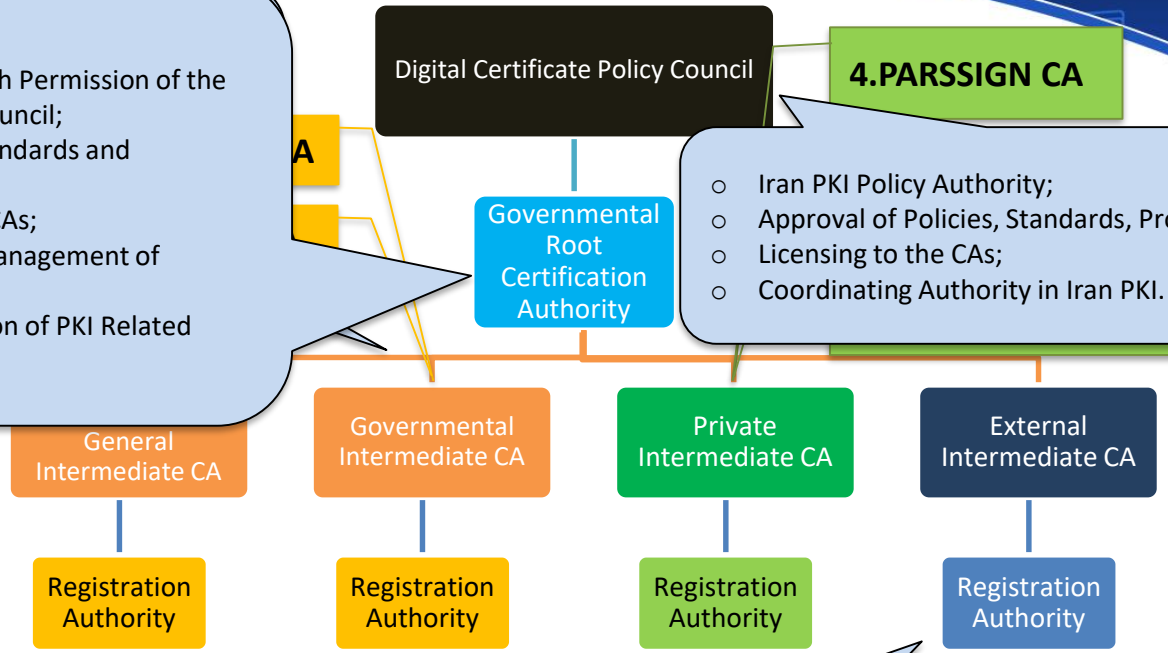
IRAN Center for
eCommerce Development

PKI Architecture, Usage and Application

IRAN Center for
eCommerce Development

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;
- More than 3000 Registration Authorities in Iran PKI.

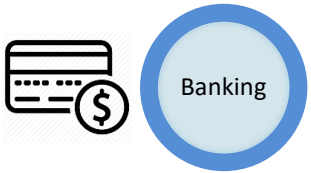
IRAN Center for eCommerce Development

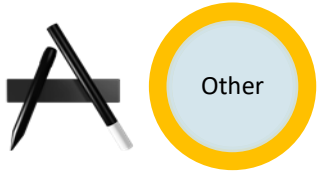
PKI Architecture, Usage and Application

IRAN Center for eCommerce Development

PKI Architecture, Usage and Application

Application Areas



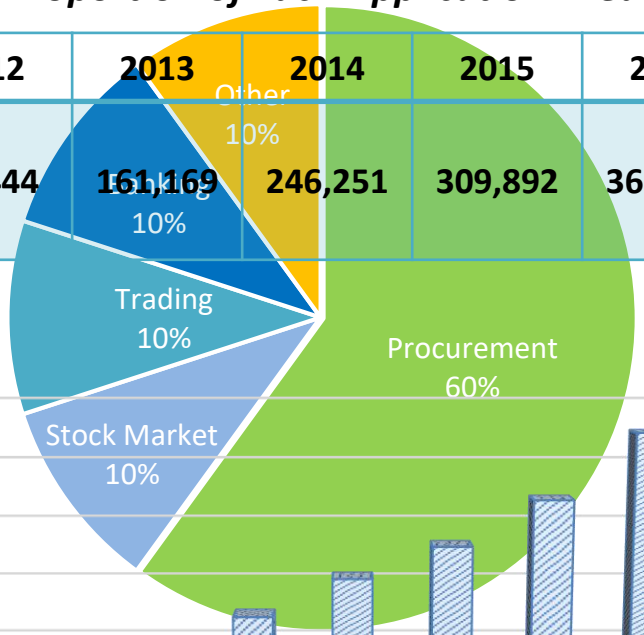


PKI Architecture, Usage and Application

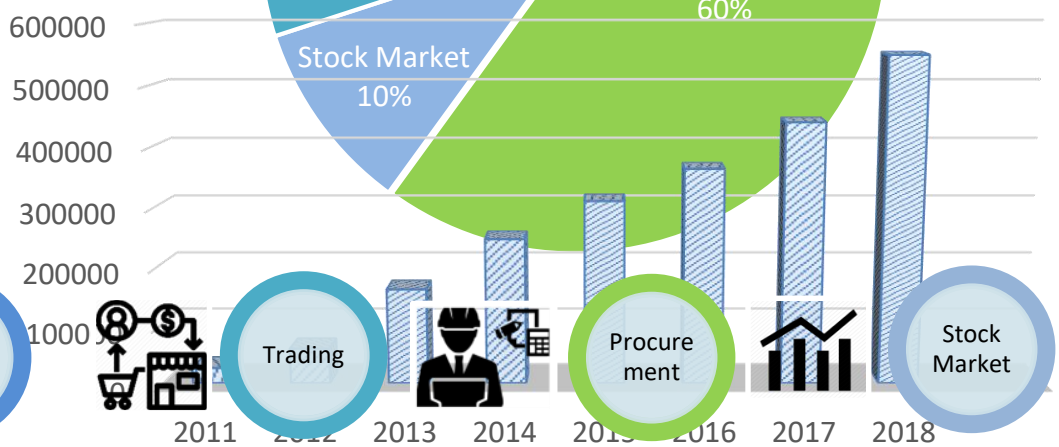
Statistics of Issued Certificates

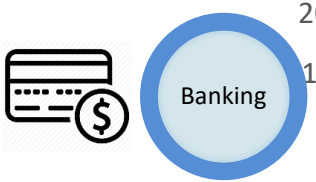
Year	2011	2012	2013	2014	2015	2016	2017	2018
Number of Issued Certificates	26,218	59,444	161,169	246,251	309,892	363,574	440,188	549,672

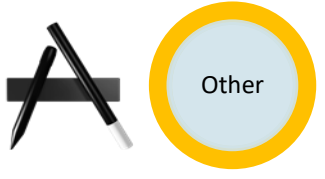
Proportion of Each Application Area



❖ Iran population: 82,792,205







PKI
Laboratory

IRAN Center for
eCommerce Development

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 Center for
eCommerce Development

PKI
Interoperability

IRAN Center for
eCommerce Development

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.

IRAN Center for eCommerce Development

THANK YOU

For Your Attention