PKI STATUS IN IRAN
Iran Center for e-Commerce Development
PKI Laws & Regulations

PKI Hierarchy, Usage and Application

Current Projects in IRAN

Future Plans
PKI Laws & Regulations

- E-commerce Law (2001)
- Executive Regulations, Article 32
- Digital Certificate Policy Approved by Policy Council
PKI HIERARCHY, USAGE AND APPLICATION
Digital Certificate Policy Council

- Governmental Root Certification Authority

- Trustee 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;
- Licensing to the CAs;

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.

Pakistan Authority;
- Approval of policies, standards, procedures;
- Coordinating authority in Iran PKI.
PKI Hierarchy, Usage and Application

- **Very High Risk Assurance Level**
- **High Risk Assurance Level**
- **Medium Risk Assurance Level**
- **Low Risk Assurance Level**

Levels:
- **Level 1**: Bronze
- **Level 2**: Silver
- **Level 3**: Gold
- **Level 4**: Platinum
PKI Hierarchy, Usage and Application

Application Areas

- eBanking
- Trading
- eProcurement
- Stock Market
- Tax
CURRENT WORKS IN IRAN
1. Update Certificate Policy (CP)

- Online identification based on 2-factor strong authentication by applying proof of presence & Liveness detection approved as identification method for Assurance Level 1

- Online identification based on 3-factor strong authentication by applying proof of presence & Liveness detection approved as identification method for Assurance Level 2
1. Update Certificate Policy (CP)-2

- Adding Encryption and System Certificates to the list of different certificates issued by ICAs
- Updating security requirements for Hardware/software security modules in all levels
- Reducing CRL issuance and publications intervals
- Mandating ICAs to provide OCSP Services for all the certificates issued in all assurance levels
New Services/Organization Using Digital Certificates

- E-health (Digital Patients’ records and digital prescription)
- Trade Single window (Comprehensive System)
- Road Bill Of landing System
- Loans and facilities Payment
- Digital Cheque/Promissory notes
- TAX
FUTURE PLANS
Future Plans

Our Next Steps

Development of an integrated system with the cooperation of private sector to produce electronic documents, digital signing of the documents and verification and validation of signed ones.

Developing the use of Digital Signature in different areas such as custom services, educational services such as providing certificates, ...

Developing and Empowering of Intermediate CAs, especially private ICAs
THANK YOU
FOR YOUR ATTENTION