



# Public Key Infrastructure (PKI)



1st Expert Group Meeting (EGM) on Electronic Trade-ECO Cooperation on Trade Facilitation

23-25 May 2012, Kish Island, I.R.IRAN

- ⇒ Part I: Introduction
- ⇒ Part II: Public key infrastructure
- ⇒ Part III: PKI status in IRAN





# *Introduction*





Merchant and Customer perform a transaction on digital world



## Paper report

Environment Agency

Business Name e Compliance, Inc

Chemical N-Methyl-N-Nitroso-Guanine

Amount at hand 0.010 Units Kg

I certify the above information is correct and take personal responsibility for any inaccuracies contained herein

Signature Bijan Fouladi

Name BIJAN FOULADI

Title VP, Environmental Affairs

## Digital report

Business Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Environment Agency

Business Name

Chemical

Amount at hand  Units

I certify the above information is correct and take personal responsibility for any inaccuracies herein

Responsible Individual

Title

Done My Computer

## Digital Signature

Ensuring **Authenticity** and Report **Integrity**  
in Electronic Transactions



There is still a problem related to the  
“*Real Identity*” of the *Signer*.

*Why should I believe the Sender claims to be?*

**Digital Certificate**



*Moving towards PKI ...*



## CERTIFICATE

Issuer

Subject

Subject Public Key

Issuer Digital  
Signature

• Issuer (CA) Distinguished Name (DN) e.g.  
C=GB, O=Baltimore Technologies, OU=PSD

• Serial number (allocated by CA)

• Validity period (typically a year)

• User (Subject) Distinguished Name

• User Public Key parameters e.g. RSA

• User Public Key

• Extensions e.g.

- Alternative user name (e.g. e-mail address)
- Key usage e.g. digital signature, key encipherment

• Signing algorithm parameters  
e.g. SHA-1, MD5

• CA Signature



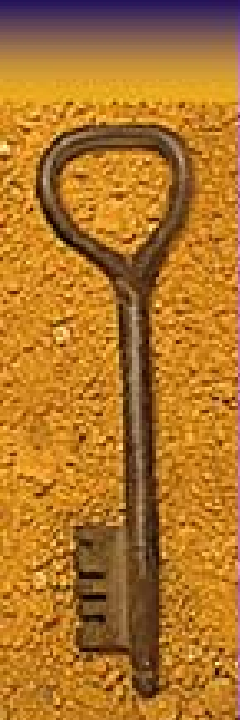
## Challenges:

- How are Digital Certificates Issued?
- Who is issuing them?
- Why should I Trust a Certificate Issuer?
- How can I check if a Certificate is valid?
- How can I revoke a Certificate?
- Why are we using Certificates?

**Public key Infrastructure**



*Moving towards PKI ...*



# Public Key Infrastructure (PKI)



PKI is an Infrastructure to support  
and manage Digital Certificates



## *Basic Components:*

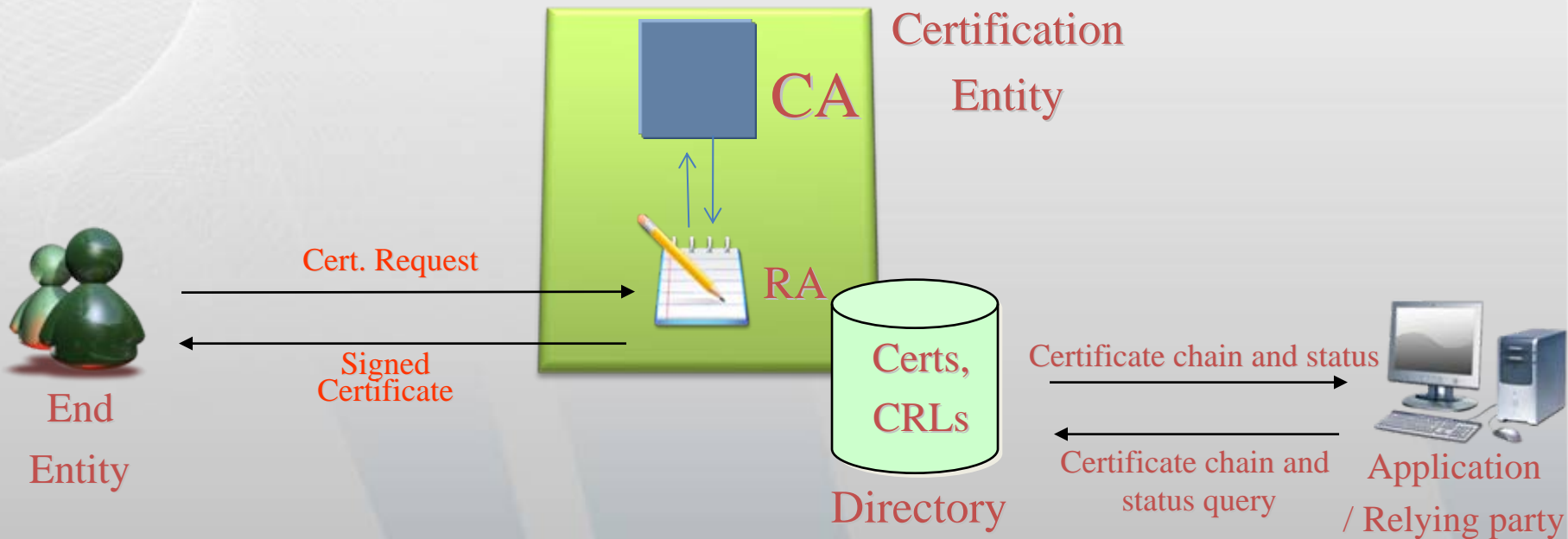
- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Distribution System
- PKI enabled applications



**“Provider” Side**

**“Consumer” Side**

# PKI – Simple Model





# PKI Status In IRAN



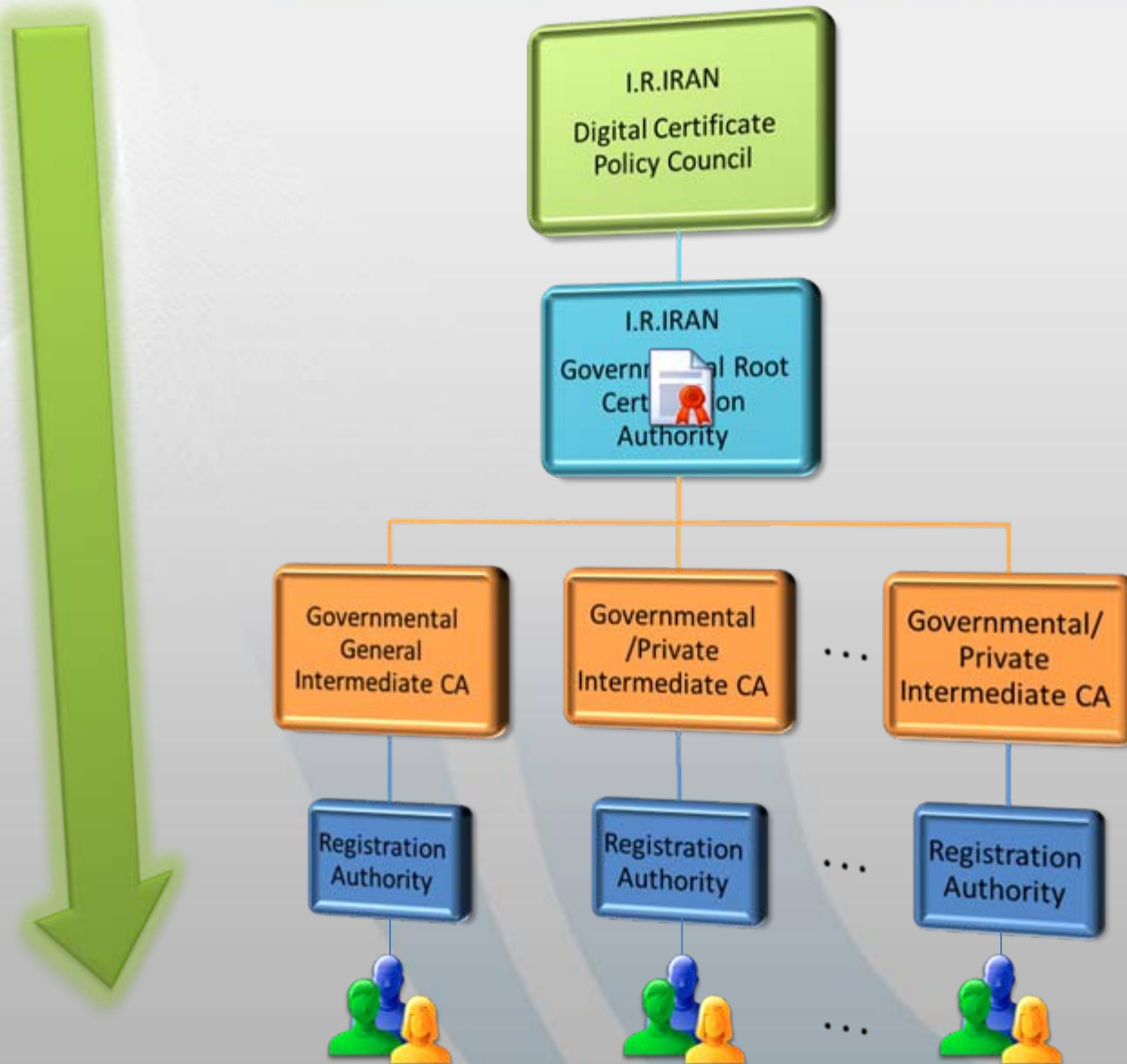
- **E-Commerce Law**

- **Article 32 of e-commerce executive regulation**

- **Certificate Policy**

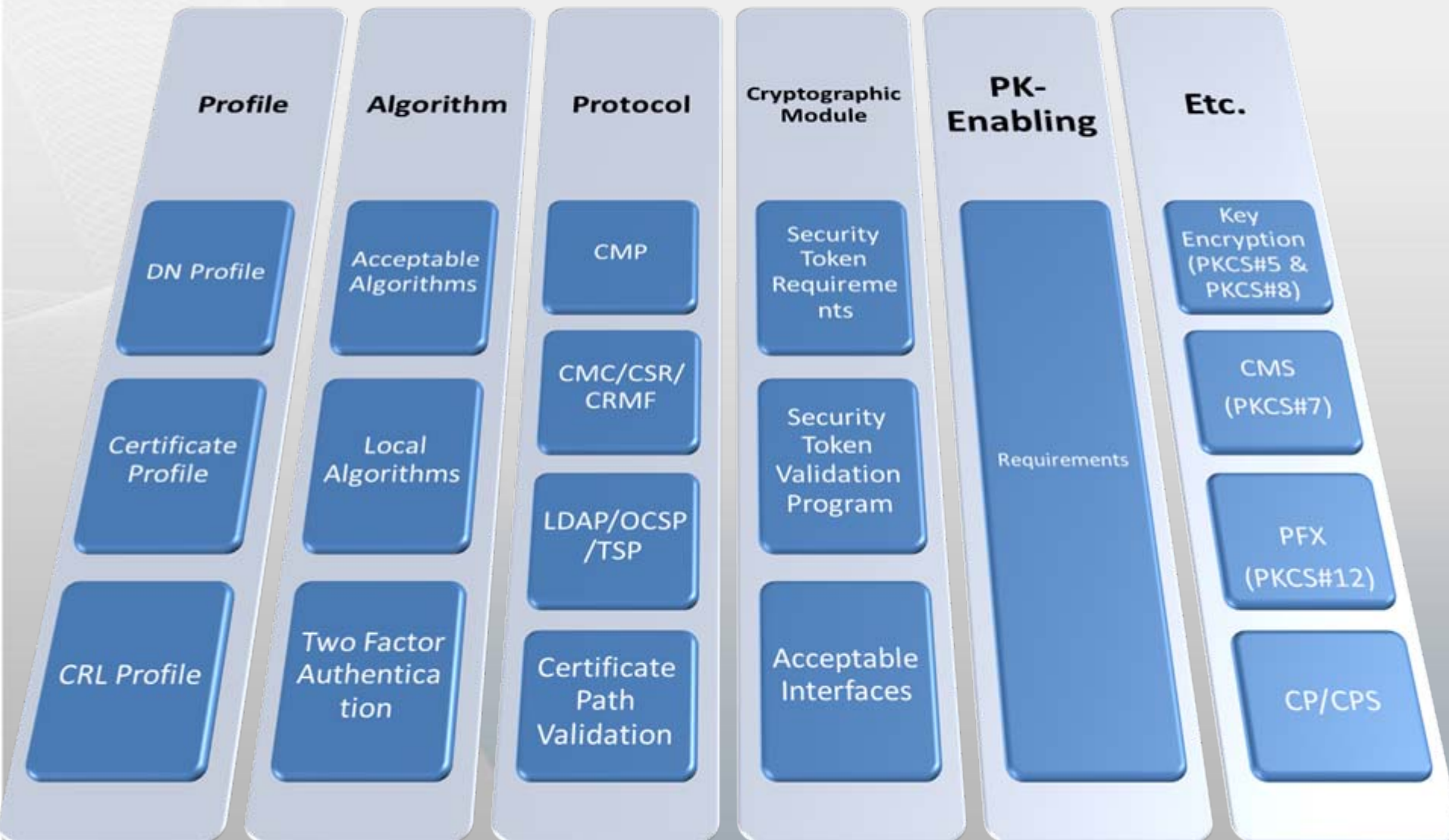








# IRAN PKI Standards





- **HSM Laboratory:** for testing and evaluation of **Hardware Security Modules**

- ✓ Smart Card
- ✓ USB Token
- ✓ HSM (internal/External)



- **CA Laboratory:** for testing and evaluation of digital certificates issuing and managing products

- ✓ CA, RA, OCSP, TSA, ...



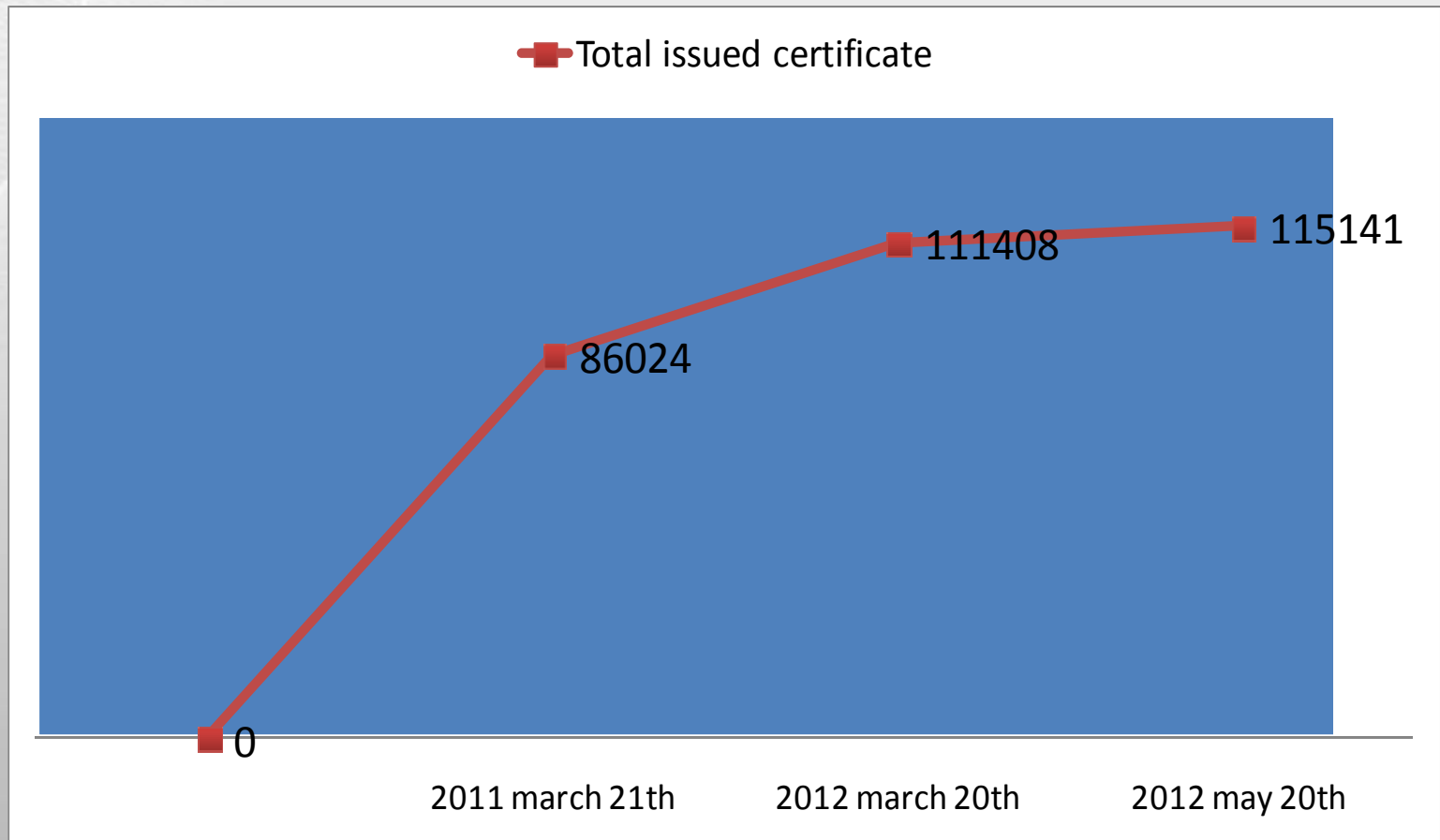
- **PKE Laboratory:** for testing and evaluation of **PK-enabled applications**

- ✓ Web based Applications
- ✓ Stand alone Applications

- **Cryptology Laboratory:** for testing and evaluation of **Cryptographic Algorithms**

- ✓ cryptographic algorithms (Symmetric, Asymmetric , ...)





# *PKI Interoperability Experiences*



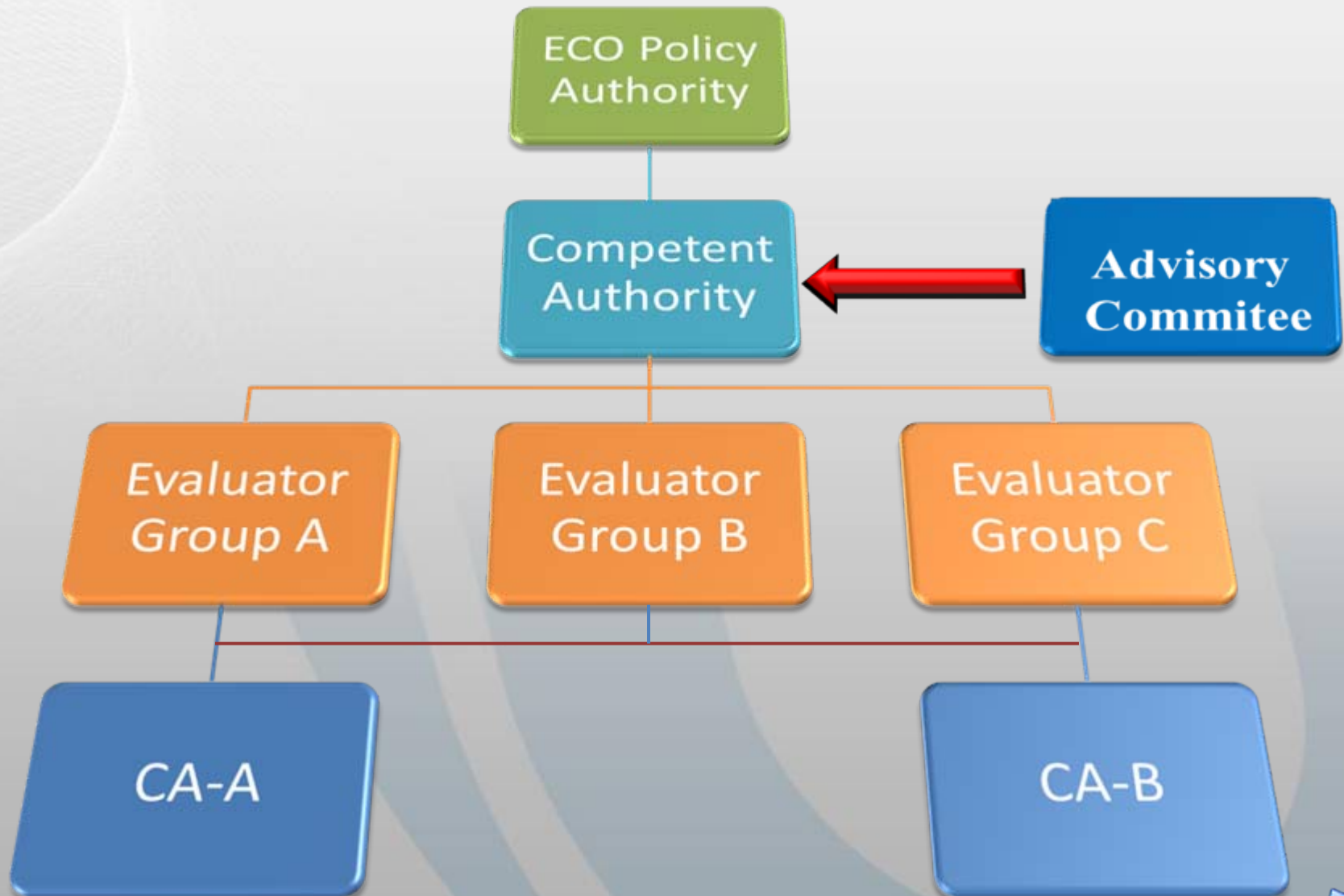


- ➔ Usability of legal digital signature in different PKI domains
- ➔ ensuring that the certificates meet *assurance requirements* and have legal effect as required
- ➔ activate *global e-commerce*
- ➔ exchanging PKI related information between the different domains

And finally:

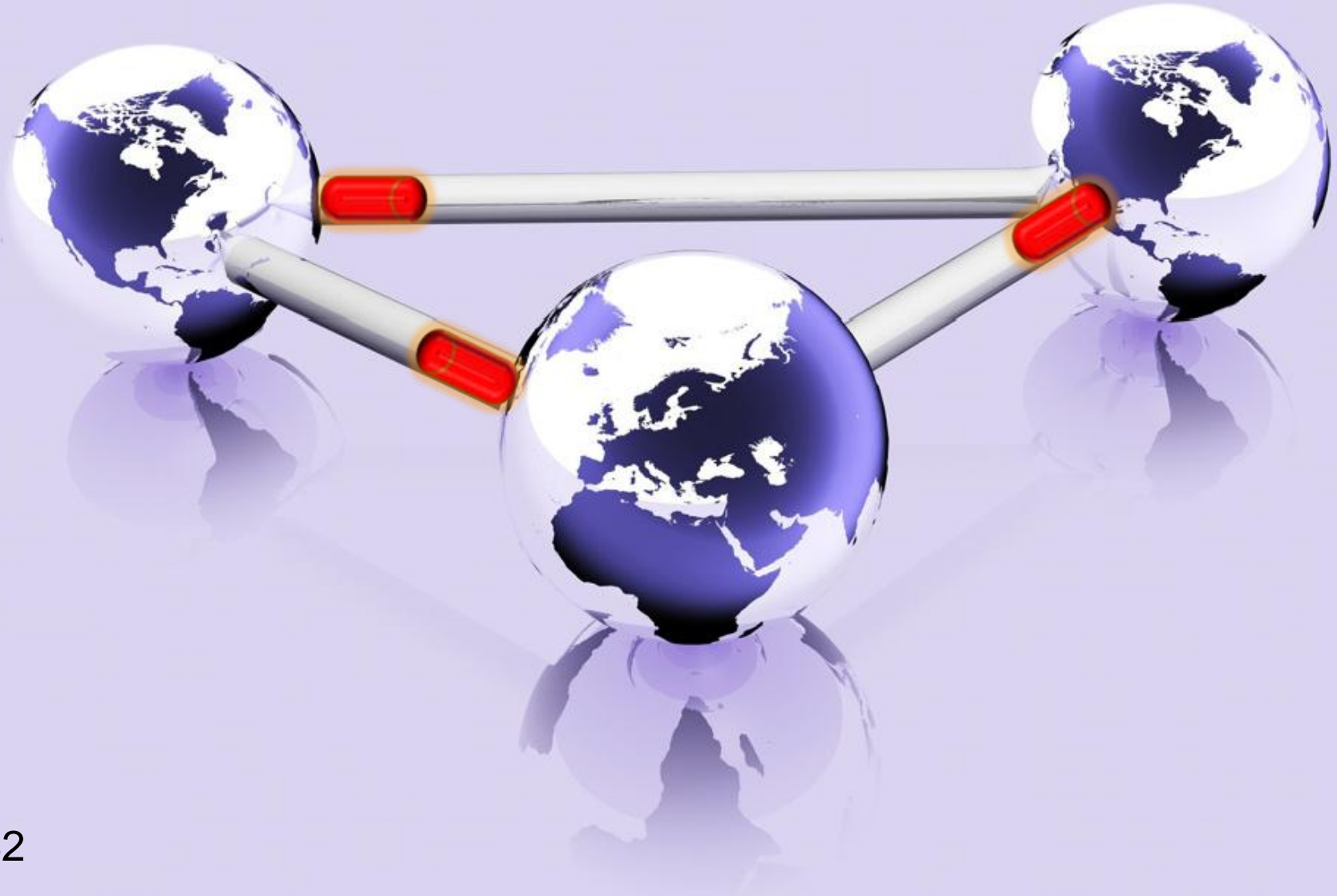
Establish trust in cross border transactions



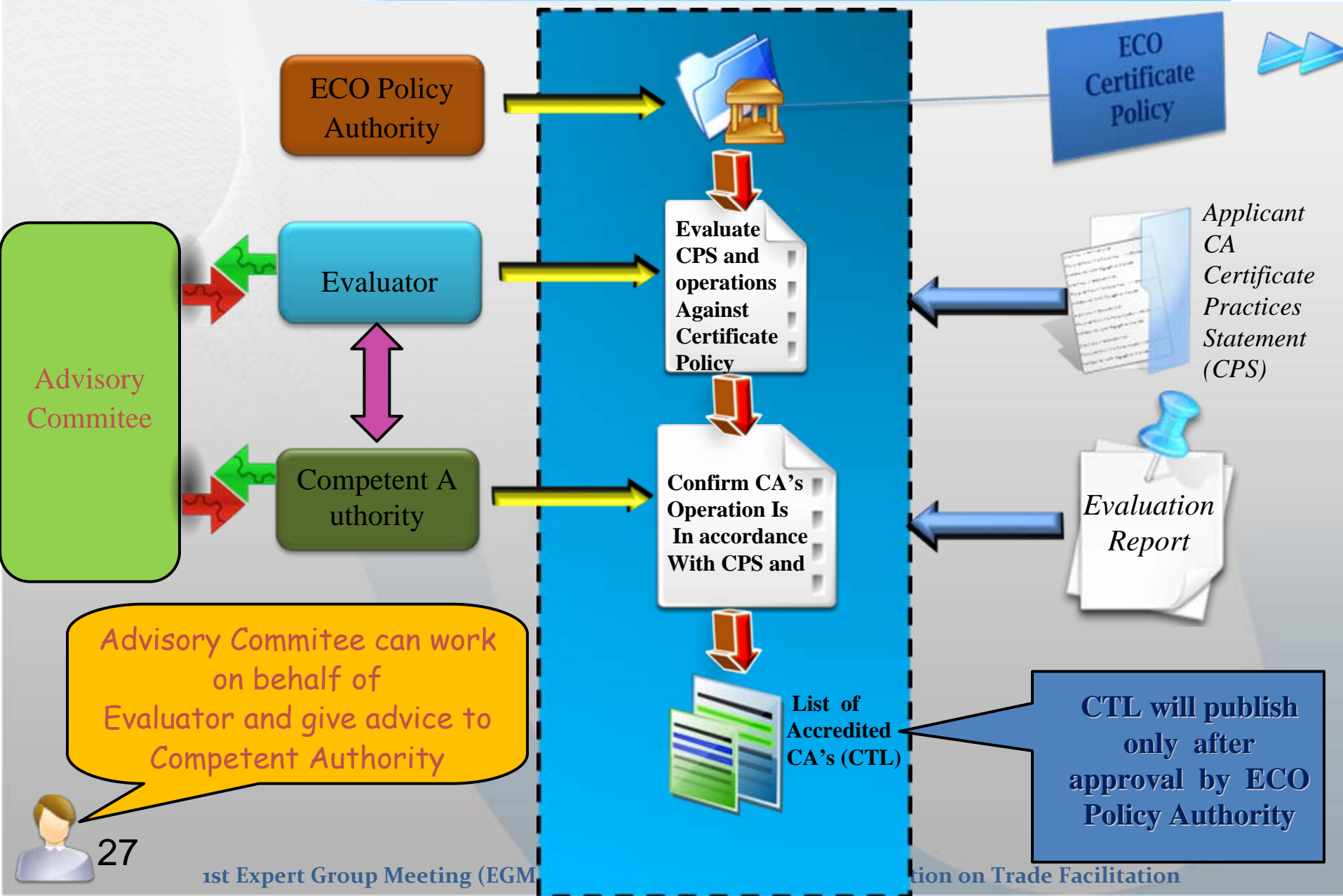


# IRAN Root CA Scheme for PKI Interoperation

## Cross Recognition + CTL



# Recommended PKI Mutual Recognition



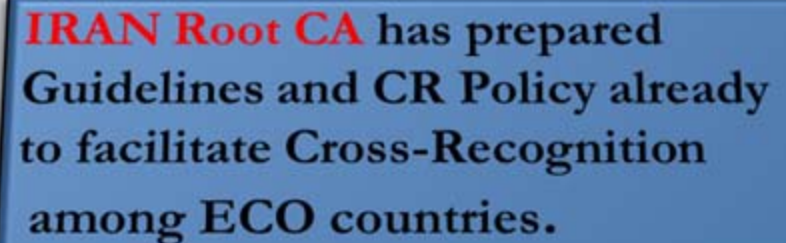


- Consulting services for **Design** and **establishing** of **Interoperation Scheme** in ECO PKI Domains
- Provide advice and services to **establishing PKI domain** for ECO members
- Consulting services for **integrating** of PKI Domains
- Provide **Auditing** and **Evaluation** services to Competent Authority
- Act as an evaluator** if there is no auditor in a country
- Give advice to *Competent Authority* for **policy compliance Auditing**, evaluation guidance, criteria and standards.



According to I.R.IRAN Root CA recent efforts, it can operate as Advisory Committee to facilitate Cross-Recognition procedure between ECO countries.

- Established of Hierarchical PKI Domain with **four levels policy**
- Established of **PKI Laboratories** for Auditing purposes
- Providing of Internal **PKI Standards** in order to create of Interoperation
- Design an **optimal scheme** for interoperability in PKI
- Preparation of **CP Guidelines** in order to providing of a template and guidance for ECO Certificate Policy Edition
- Preparation of **CR Policy** in order to propose the Architecture and mechanisms of cross-recognition



**IRAN Root CA** has prepared Guidelines and CR Policy already to facilitate Cross-Recognition among ECO countries.





Thanks for your attention