



# 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

# Outline

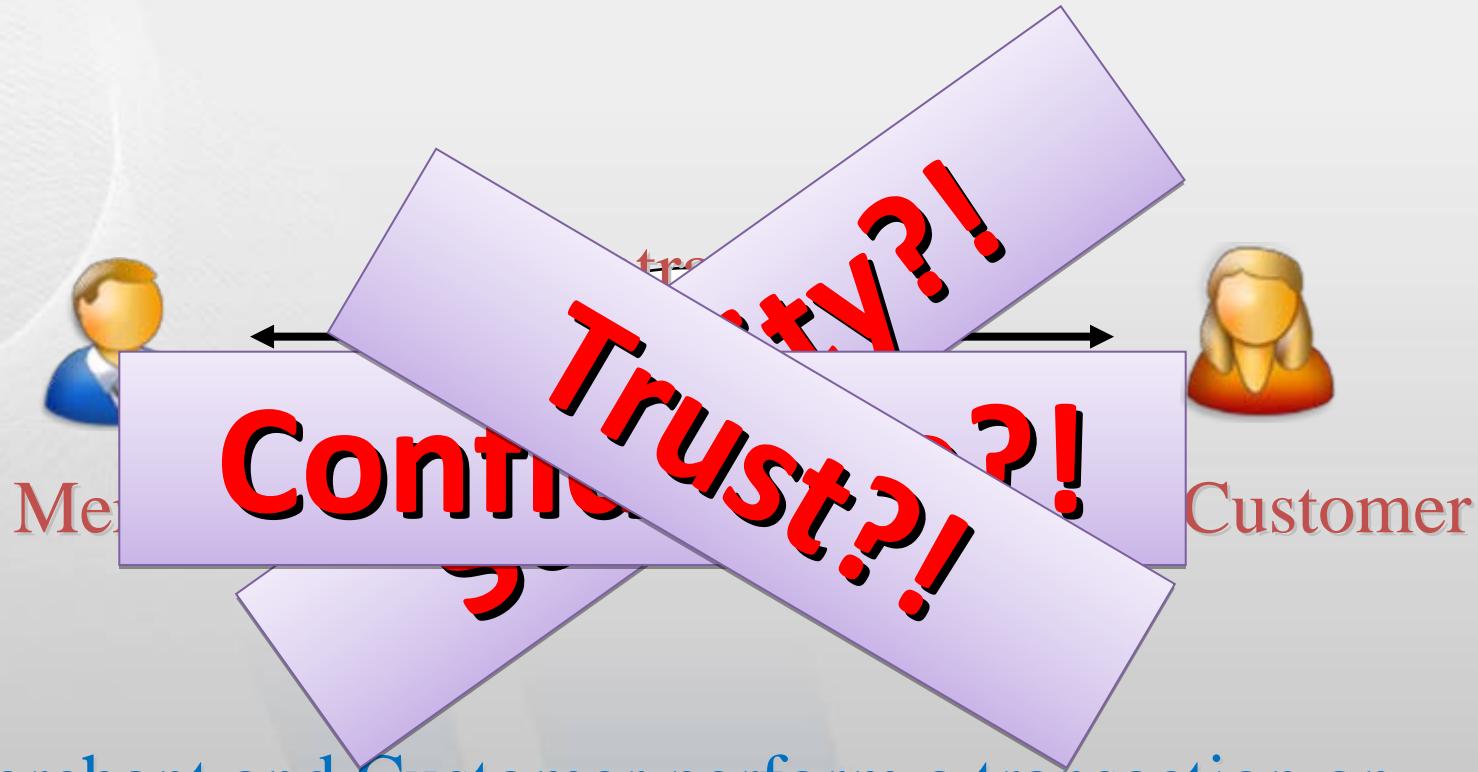
- ➡ **Part I: Introduction**
- ➡ **Part II: Public key infrastructure**
- ➡ **Part III: PKI status in IRAN**





# Introduction





Merchant and Customer perform a transaction on digital world



## Paper report

Environment Agency

Business Name eCompliance, 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 → Stop × Refresh Home Search Favorites Media My Computer

**Environment Agency**

Business Name

Chemical

Amount at hand  Units

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

Responsible Individual

Title

Submit Form

Done My Computer

A large red stamp with the word "TRUST" and a question mark is overlaid on the digital form.

# Digital Signature

Ensuring Authenticity and Report Integrity  
in Electronic Transactions



There is still a problem to the

*“Real Idea”* to the Signer.

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

**Digital certificate**



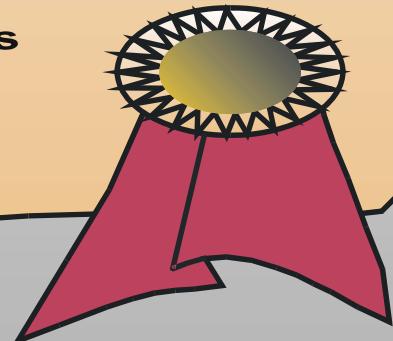
*Moving towards PKI ...*



# Digital Certificate

## CERTIFICATE

- ▶ 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



预览已结束，完整报告链接和二维码如下：

[https://www.yunbaogao.cn/report/index/report?reportId=5\\_7601](https://www.yunbaogao.cn/report/index/report?reportId=5_7601)

