ICTA
Information and Communication
Technologies Authority

E-signature, M-signature, Registered E-Mail in e-APP Turkey Project

Mustafa ÜNVER
Head of Information Technologies Department

7th International Forum on the e-APP

15 June 2012, İzmir

Agenda

- Introduction

- Electronic signature

    - What is e-signature? Elektronik İmza Nedir ?

    - Regulatory framework in Turkey

    - M-signature

    - Market overview in Turkey

    - Applications

- Registered E-mail (REM)

- e-APP

- Conculusions

Introduction

➢ **Development of information and communication technologies**

INTEGRITY

AUTHENTICITY

NON-REPUDIATION

NEEDS :

- **Security**
- **Reliability**
- **Legal validity**

⇒ **e-signature**

7th International Forum on the e-APP, İzmir 2012

3
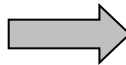
What is e-sign?

Definition

"data in electronic form that are attached to other electronic data or linked logically to that electronic data and used for authentication" **(E-sign Law/ Article 3)**

Power of E-sign

❑ Secure electronic signature shall have the same legal effect with handwritten signature. (Law-Art.5)

❑ Electronic data that are generated with secure electronic signatures in accordance with procedures are equivalent to bill.(Law-Art.23)

❑ Exceptions:
A secure electronic signature shall not be applicable to legal proceedings subject to a special procedure or an official form pursuant to laws and warranty contracts. (Law-Art.5)
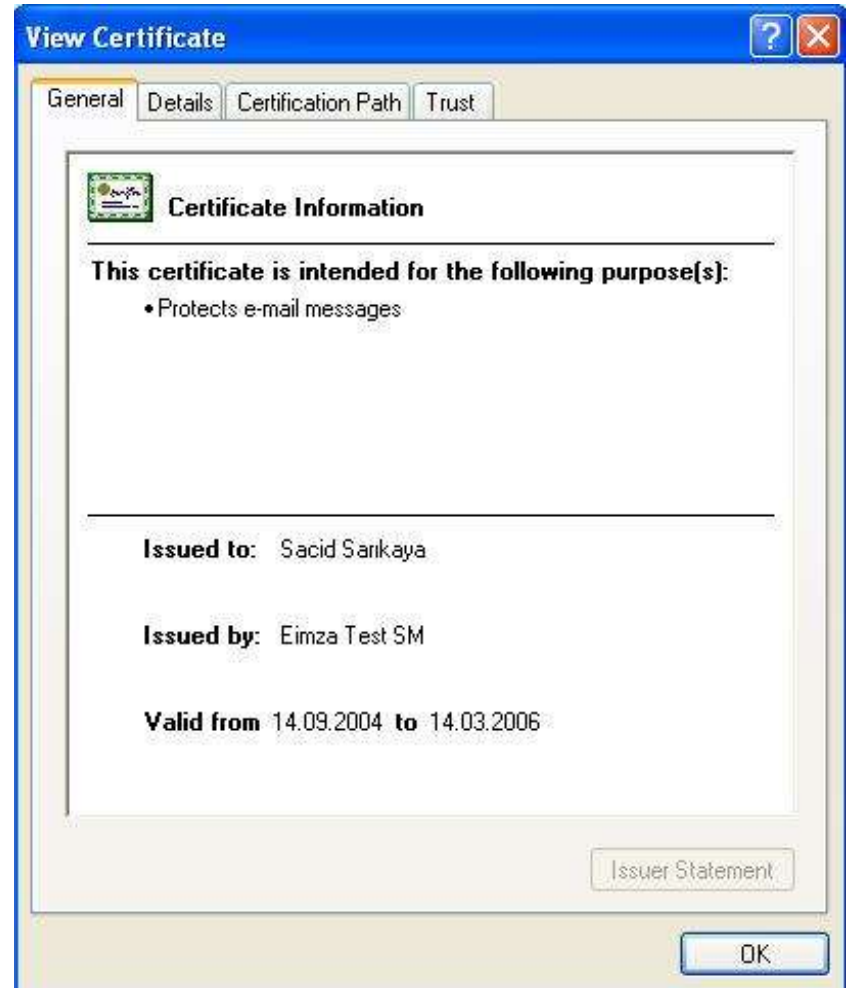
Secure E-sign

- ❑ "Secure" e-signature (Law, Art.4):
  - ❑ is exclusively assigned to the owner of signature
  - ❑ is generated with the secure electronic signature creation device
  - ❑ which is kept under sole control of the signature owner
  - ❑ enables the identification of the signature owner based on the qualified electronic certificate
  - ❑ enables to detect whether signed electronic data is altered or

Electronic Certificate

Electronic data binding the signature verification data of the signature owner to identity data of that person (Law, Art.3)

View Certificate

General | Details | Certification Path | Trust

Certificate Information

This certificate is intended for the following purpose(s):
- Protects e-mail messages

Issued to: Sacid Sarıkaya

Issued by: Eimza Test SM

Valid from 14.09.2004 **to** 14.03.2006

Issuer Statement

OK

Qualified Electronic Certificate

- ❑ It is required that Qualified Electronic Certificates shall include the following;
    - ❑ an indication that the certificate is a "qualified electronic certificate",
    - ❑ the identity information of the Electronic Certificate Service Provider and the country in which it is established,
    - ❑ the identity information by which the Signature Owner can be identified,
    - ❑ Signature-Verification Data which correspond to Signature-Creation Data,
    - ❑ the date of the beginning and the end of the validity period of the certificate,
    - ❑ serial number of the certificate,
    - ❑ the information regarding the authorization of the certificate holder if the holder acts on behalf of another person,
    - ❑ when the certificate holder so requests, occupational and other personal information,
    - ❑ information related to conditions of the usage of the certificate and limits on the value of transactions, when applicable,
    - ❑ the Secure Electronic Signature of the electronic certificate service provider that verifies the information in the certificate. (Law, Art.9)

7th International Forum on the e-APP, İzmir 2012

Electronic Certificate

View Certificate

General | Details | Certification Path | Trust

Certificate Information

This certificate is intended for the following purpose(s):

• Protects e-mail messages

Certificate usage purpose

Issued to: Sacid Sarıkaya

Issued by: Eimza Test SM → Certificate Service Provider

Valid from 14.09.2004 to 14.03.2006 → Validity period

Issuer Statement

OK

View Certificate

General | Details | Certification Path | Trust

Show: <All>

Field	Value
Subject	Sacid Sarıkaya, Users, eimza, t...
Public key	RSA (1024 Bits)
Subject Alternative Name	RFC822 Name=sacid@eimza.test
CRL Distribution Points	[1]CRL Distribution Point: Distrib...
Authority Information Access	[1]Authority Info Access: Acces...
Key Usage	Digital Signature, Non-Repudiat...
Thumbprint algorithm	sha1
Thumbprint	f1 d9 59 ac 18 dc 9b d9 76 83 ...

```
30 81 89 02 81 81 00 b3 7f 57 14 35 b5 92
69 b9 e4 c4 33 d0 70 11 7e 6b 6d 16 84 30
8b 8b 94 3e ea 3a 13 0b 1b af d6 a4 cd 0f
65 6b e1 aa 85 e8 4c 72 96 0f fd 75 37 cc
da e3 1f 52 c4 9b 9e 98 fc 3d 87 42 5a d9
b4 2f fb f1 f3 1e 0e eb 3e 81 26 02 47 4d
51 ec 86 d9 b7 9a 55 a0 59 30 5e a3 bb 27
b0 b7 e4 8d b2 f7 b0 d6 db 8c e5 de a5 0e
fa 0e 8f d8 33 de eb d7 32 20 fc 0c b6 63
```

Edit Properties... | Copy to File...

OK

Public key

CSP Access address

Key usage fields

Regulatory Framework

23 Jan 2004	E-Sign Law (5070) published in Official Journal
23 July 2004	Law entered into force
23 Jan 2005	Due date defined for the preparation of secondary regulations by ICTA

Subject of Secondary Regulations

❑ ICTA is responsible from supervision of the market and publishing regulations

- ❑ Secure e-signature creation devices (SSCD)
- ❑ Secure e-signature verification devices (SSVD)
- ❑ Electronic certificate service providers (CSP)
- ❑ Liabilities of CSPs
- ❑ Revocation of qualified e-certificates
- ❑ Foreign e-certificates
- ❑ Certificate Financial Liability Insurence

Secondary Regulations for E-sign

By-law on the Certificate Financial Liability Insurence	26 Agu 2004
Prime Ministry Circular numbered 2004/21	06 Sep 2004
By-law on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (updated 2 times)	6 Jan 2005
Communiqué on Processes and Technical Criteria Regarding Electronic Signatures (updated 5 times)	6 Jan 2005
Board Decision on Security requirements for signature creation and verification applications and electronic signature format	1 June 2006
Board Decision on Qualified Electronic Certificate, CRL and OCSP Message Profiles Guide	18 April 2007

By-law on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law

ICTA — Information and Communication Technologies Authority

- ❑ CSPs notify ICTA for starting their operations
  - ❑ notification ≠ authorization
- ❑ ICTA examines notification in 2 months at most
  - ❑ Compliance with requirements stated in Annex of the By-law
- ❑ CSP commences its operations
- ❑ Certification Proses:
  - ❑ Application
  - ❑ Issuence
  - ❑ Publication
  - ❑ Renewal
  - ❑ Revocation
- ❑ Inspection
- ❑ Termination of operations (by ICTA or by CSP itself)

E-sign Application

Personal application

Real persons apply CSP(physical presence during the identity check is required)

Organizational application

Organizational applicant shall provide the qualified electronic certificate requests of the persons on behalf of whom it applies for in a written form.

Generation of Electronic Certificate

Natural Person

Application

Certificate Service Provider

Info of Person

Name, Surname
ID No

Administrative Info

CSP Name,
Validty Period,
Usage Field

Info Related to e-Signature

Public Key

Secret Key

Electronic Certificate

Delivery

Ad Soyad
TC Kimlik No

Info of Person

Administrative Info

CSP Signature

7th International Forum on the e-APP, İzmir 2012
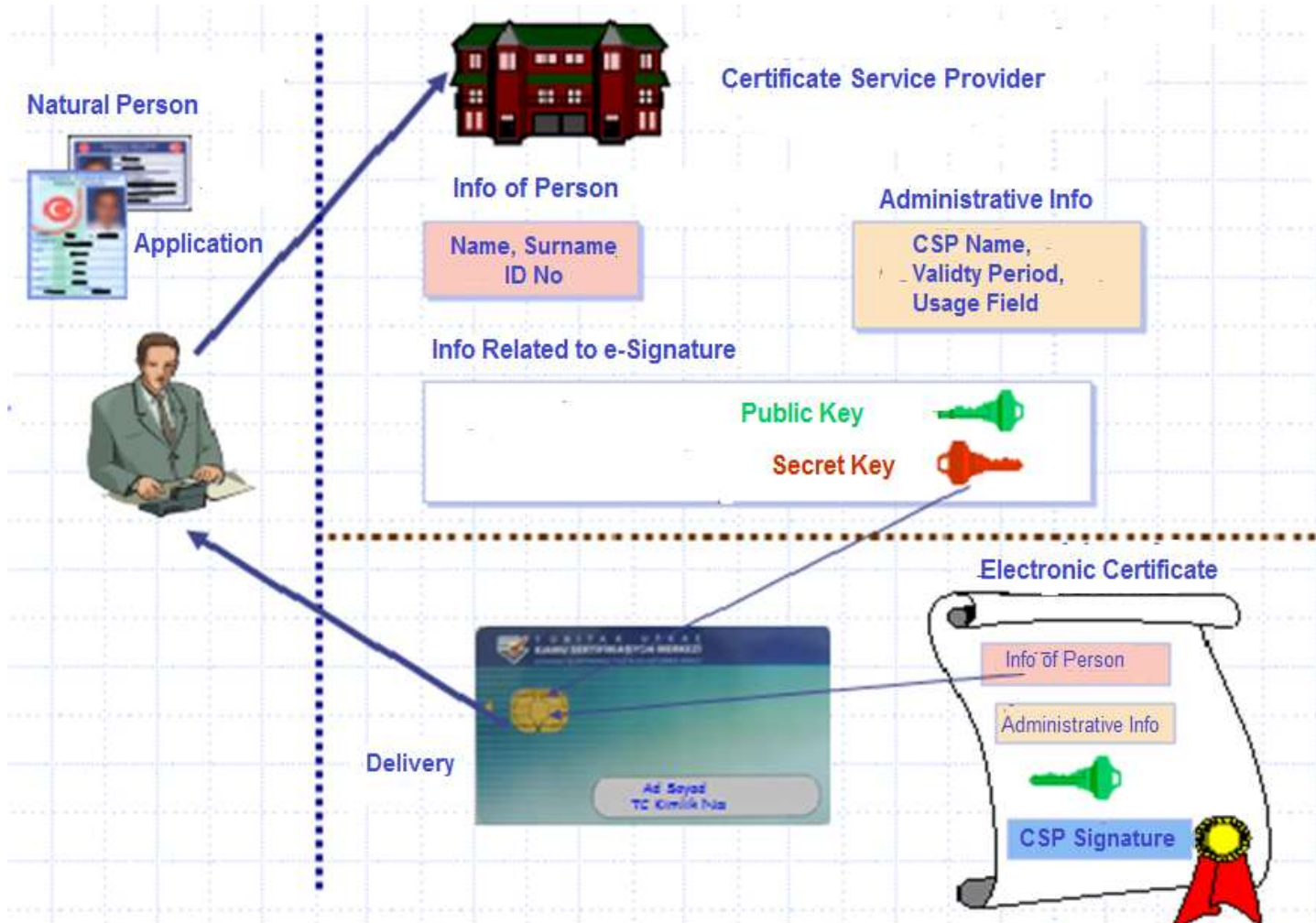
Obligations of Qualified Electronic Certificate Holder

❑ Submitting information accurately and completely to the CSP that's necessary to get qualified electronic certificate,

❑ Informing the CSP immediately in case of any change in the information submitted to CSP,

❑ Using algorithms and parameters determined by the Communiqué, in case the certificate holder generates his/her own signature creation data,

❑ Using the signature creation and verification data only for creating and verifying electronic signature and in accordance within the limitations about the usage and value of the qualified electronic certificate,

❑ Not allowing third parties to use his/her signature creation data and taking necessary cautions for this purpose,

❑ Notifying the CSP immediately in case the confidentiality or security of the signature creation data is under suspicion,

❑ Using secure electronic signature creation device,

❑ Assuring the necessary cautions in case the signature creation and verification data are generated out of the premises of CSP and with devices that do not belong to the ECSP,

❑ Informing the CSP immediately in case the signature creation device or the activation data of the signature creation device is stolen, lost or suspected to be compromised.

7th International Forum on the e-APP, İzmir 2012

Obligations of Third Parties

❑ Verifying if the certificate is qualified electronic certificate or not,

❑ Verifying the validity and revocation status of the qualified electronic certificate or using secure electronic signature verification device,

❑ Verifying if there is any limitation on the usage of the qualified electronic certificate.

Foreign electronic certificates

- International Agreements : legal results of foreign certificates are subject to and governed by the international agreements (Law-Art.14)

- Foreign Certificates Accepted by a Turkish Provider : considered and treated as "qualified electronic certificates" (Law- Art.14)
  - Foreign electronic certificate shall bear the technical criteria of qualified electronic certificate stated in the Law and in this By-Law.
  - Foreign ECSP shall operate as ECSP in the country it has been established.

(By-Law, Art. 32)

Communiqué on Processes and Technical Criteria Regarding Electronic Signatures

Operations of CSP	ETSI TS 101 456 & CWA 14167-1
SSCD	CWA 14169 & EAL4+
SSVD	CWA 14171
QEC	ETSI TS 101 862 & ITU-T Rec. X.509 V.3
Sign. Creation and Verification Data of Signatory	1024 bits for RSA or DSA or 163 bits for ECDSA Up to 31/12/2012
CP & CPS	IETF RFC 3647
Time Stamp	ETSI TS 102 023, ETSI TS 101 861
ECSP Certification	ISO/IEC 27001

7th International Forum on the e-APP, İzmir 2012

Public Certification Center

■ Prime Ministry Circular No. 2004/21, 6th Sep 2004, For the establishment of Public Certification Center under TUBITAK

■ All ministries and government offices shall obtain their certificates from TUBITAK

■ Rationale of the Circular:

■ to decrease many unnecessary and dublicative investments in the public sector

■ to achieve interoperability among different hardware and software used for electronic signature applications in the public sector.

Model in Turkey

Information and Communication Technologies Authority

Root CSP – Public CA

Public CA   Police CA   Air Forces CA

Commercial CSP   Commercial CSP

Banks, etc

P. Ministry   Health Mini.   Police   A. Forces

Employees   Employees   Police Officers   Employees

Citizens
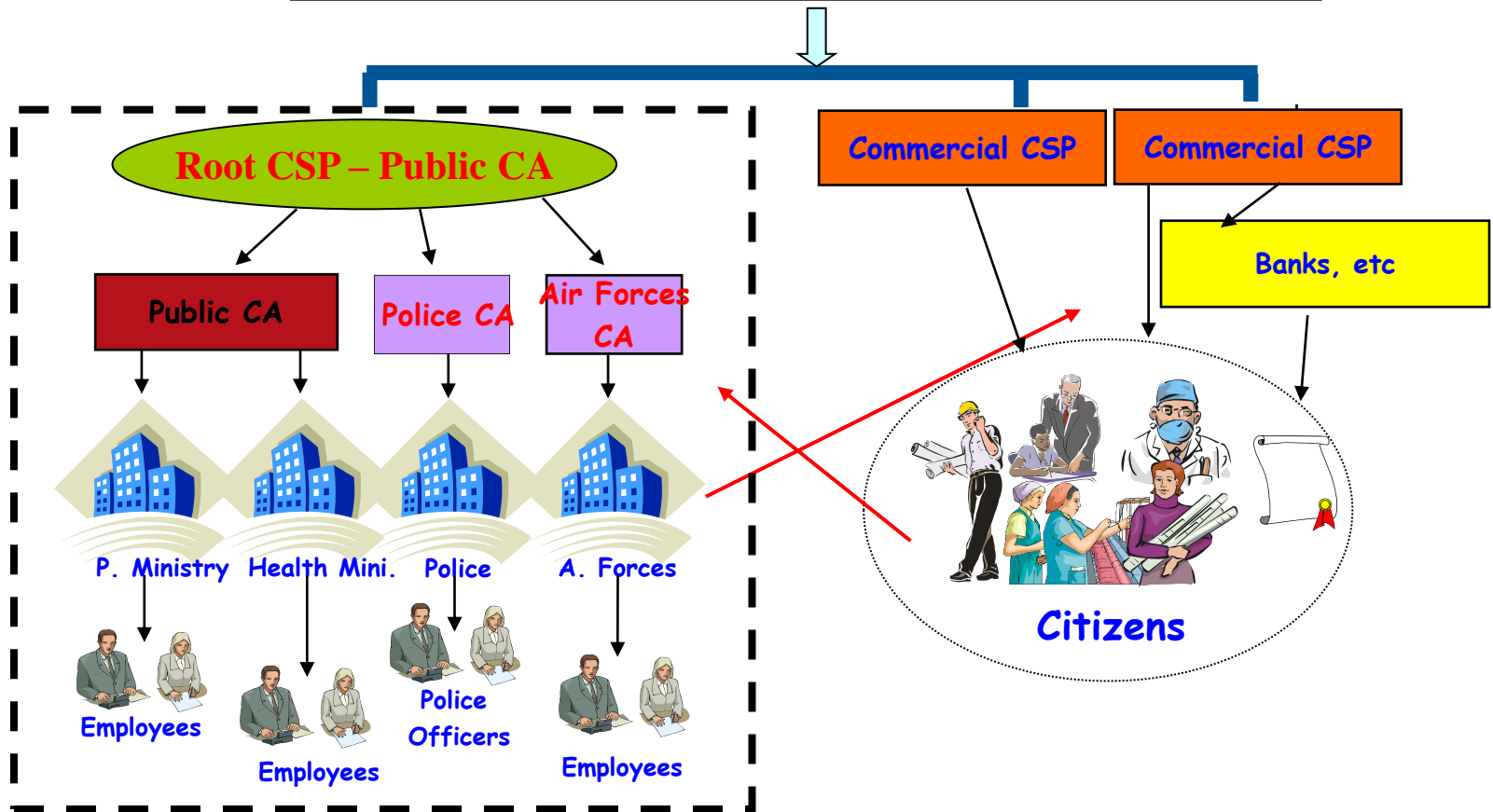
M-Signature

Why m-sign?

❑ New data platforms like GPRS added to WAP technology providing content on mobile devices enabled many applications like:

    ❑Mobile

    ❑Mobile   **MOBILE ELECTRONIC SIGN**

    ❑Mobile   **MOBILE PKI**

❑ Diffusion of businesses in mobile media makes TRUST a matter

What is M-sign?

- M-signature is an e-sign which:
  - Receives service from mobile telecom networks,
  - Is kept in a SIM card of a mobile device
  - Is generated by a secret PIN produced by cryptographic algoritm

M-signature in Turkey

❑ Feb 2007 - e-Güven (CSP) & Turkcell (Mobile Operator)

❑ Dec 2007 – Turktrust (CSP) & Avea (Mobile Operator)

m-imza uygulaması

Internet

Mobile Sign Platform

Internet

Mobile Sign Platform

M-sign diffused faster bc for users;
- **Easier to use**
- **Cheaper**

compared to conventional e-sign

1

2

23.11.06 at 19: are signing for into the inter banking application ABCD Bank. Verify signing.

OK   Back

0000 001D 0240 2A24
435B 7B02

OK   Back

Enter your PIN to sign

XXXXXX
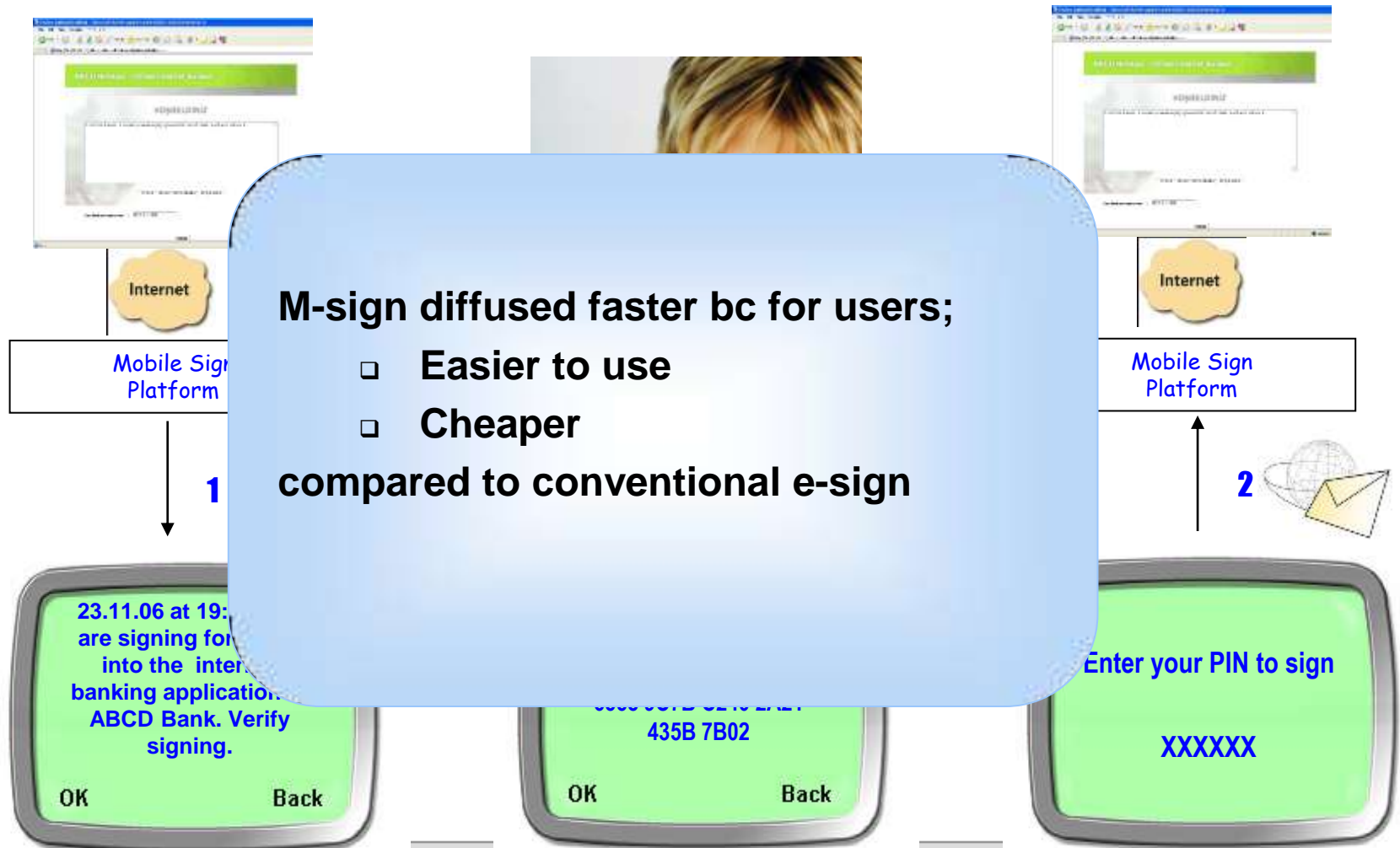
CSPs

CSP	Notification Date	Date of Starting Operations
e-GÜVEN	25.03.2005	24.06.2005
Public CA	31.03.2005	30.06.2005
TURKTRUST	13.05.2005	16.07.2005
EBG	20.06.2006	01.09.2006

7th International Forum on the e-APP, İzmir 2012

E-sign Market

Number of e-certificates issued
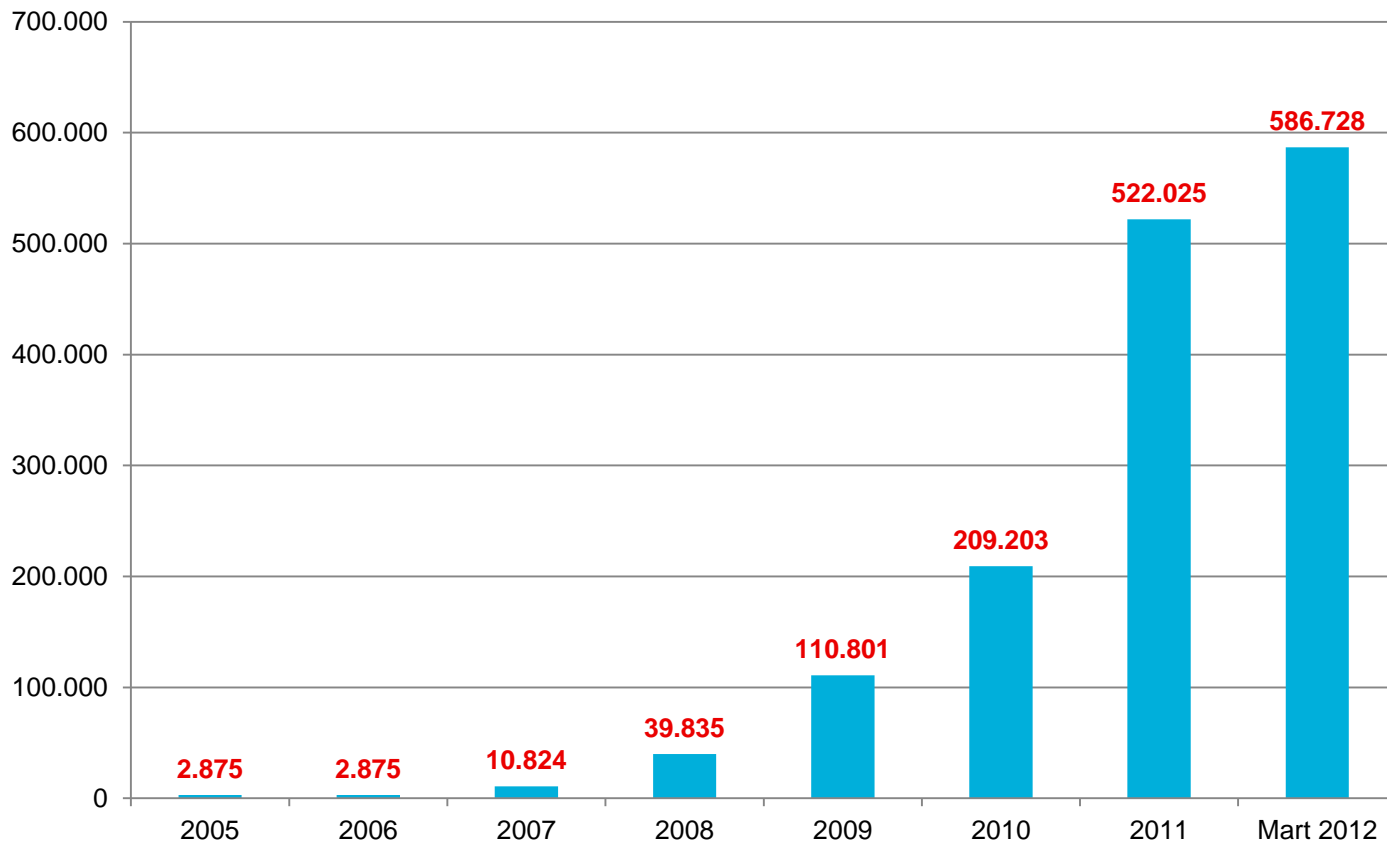
Year	Value
2005	2.875
2006	2.875
2007	10.824
2008	39.835
2009	110.801
2010	209.203
2011	522.025
Mart 2012	586.728

7th International Forum on the e-APP, İzmir 2012

E-sign Market

Chart: E-sign Market

Year	Elektronik İmza	Mobil İmza
2005	2875	
2006	10824	
2007	17.298	22.537
2008	44.777	66.024
2009	114.675	94.528
2010	201.280	113.955
2011	323.242	198.783
Mart 2012	375.089	211.639

Legend: Elektronik İmza, Mobil İmza

E-sign Market

37%

63%

- Kamu Kurum ve Kuruluşları

- Özel Sektör

* As of end of March 2012
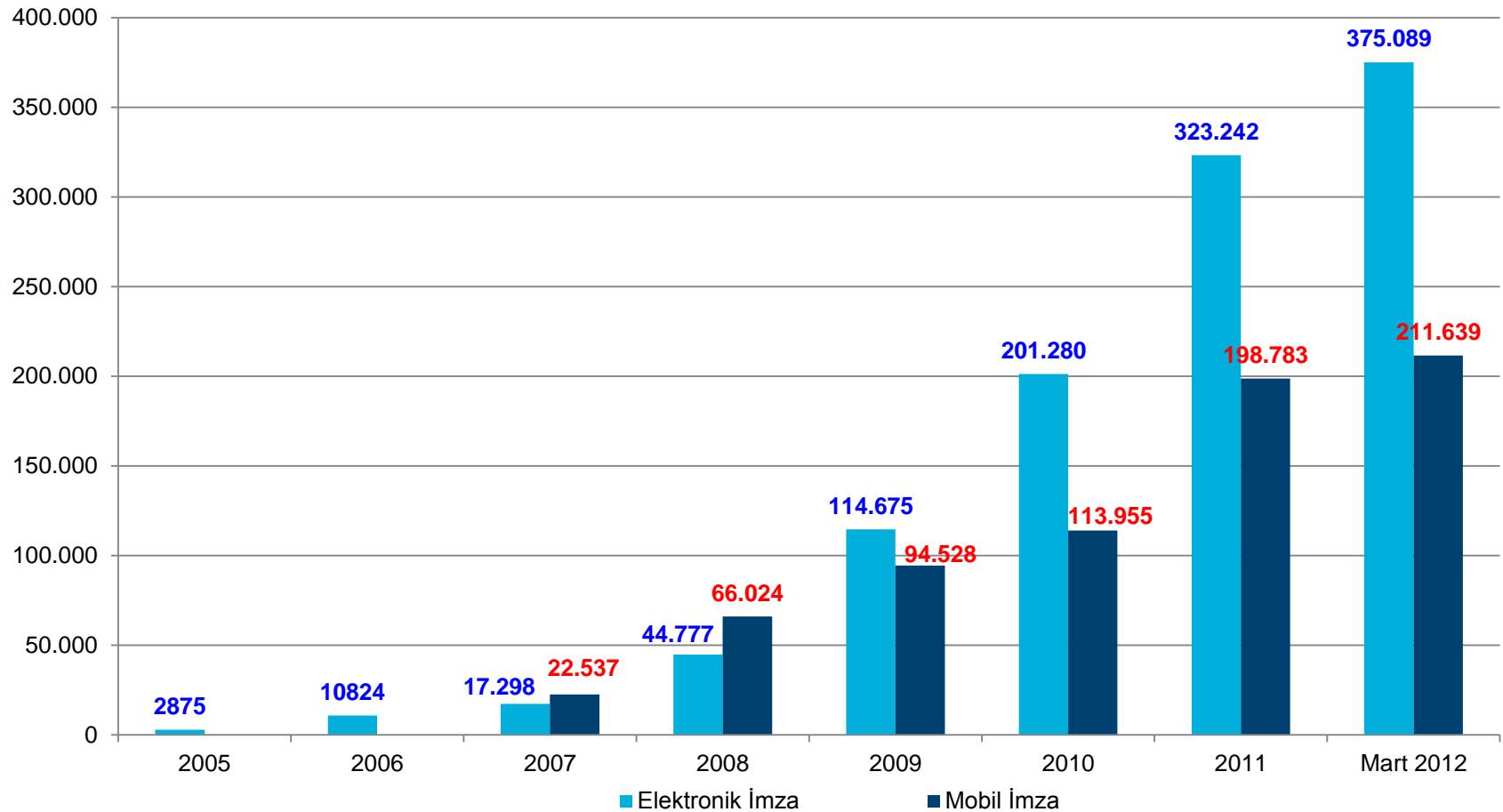
7th International Forum on the e-APP, İzmir 2012
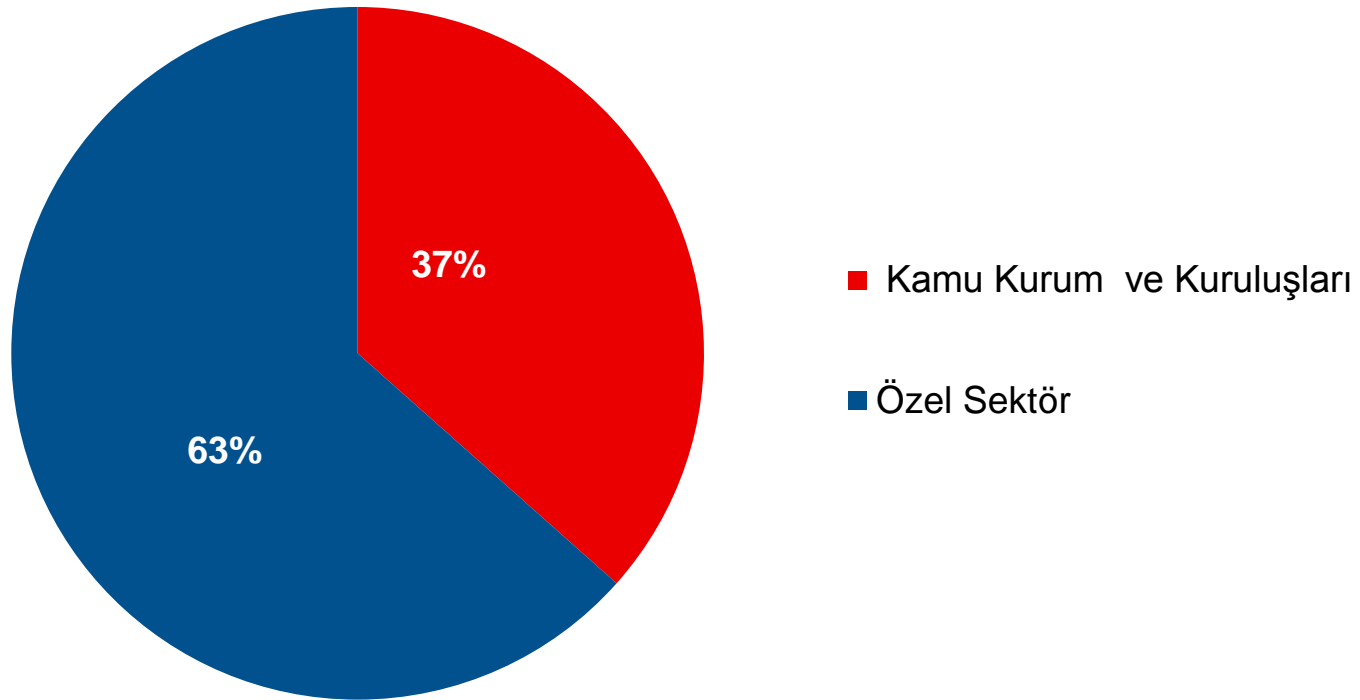
E-sign Market

As of End of March 2012	E-sign	M-sign
Number of certificates issued	375.089	211.639
Number of certificates revocated	13.641	86.589
Number of certificates which are not valid anymore	113.889	144.957
Number of certificates suspended	431	2.105

7th International Forum on the e-APP, İzmir 2012

Prices of qualified e-certificates/CSP

CSP	Price(TL)	Price(EUR)	Price($)	Yr
e-Tuğra	149,00	64,10	84,79	1
	219,00	94,22	124,62	2
	279,00	120,03	158,77	3
TürkTrust	215,00	92,50	122,35	1
	299,00	128,64	170,15	2
	379,00	163,05	215,67	3
e-Güven	110,00	47,32	62,60	1
	200,00	86,04	113,81	2
	285,00	122,61	162,18	3
Public CA	89,00	38,29	50,65	3
	109,00	46,89	62,03	5

Mobile sign: 5 TL/month, 60 TL/yr

7th International Forum on the e-APP, İzmir 2012

Application Examples

Applications

- Under-Secretariat of Foreign Trade: Internal Processing Regime and Free Trade Zone Projects

- Ministry of Justice: UYAP (National Court Network) Project

- Ministry of Trade and Industry: Guarantee Certificate Project

- Patent Institute: Mark, Patent and Design Applications

- Under-Secretariat of Customs: Customs Decleration Project

- Energy Market Regulation Authority: Petrol Market Information System

- Ministry of Finance: e-invoice

7th International Forum on the e-APP, İzmir 2012

Applications

- Ministry of Environment: E- Environment License Project

- Public Procurement Authority: Electronic Procurement Project

- E-Government Gateway

- Ministry of Health: E-transformation in Health Project (e-prescription, etc)

- National Population Registry: Address Recording System

- Ministry of Internal Affairs: Online Car Registry Project

- Many e-document and e-archival management projects in public sector

- Internet Banking: Akbank, Bank Asya, BankPozitif, Denizbank, Finans Bank, Fortis Bank, İş Bankası, Yapı Kredi, Garanti Bankası, TEB, HSBC, Şekerbank, Tekstilbank, Kuveyt Türk, Türkiye Finans

- E-Municipality applications: Eminönü, Fatih, Şişli, Zeytinburnu, Beyoğlu, Odunpazarı

Application example: E-Government Gateway

Application example:
E-Government Gateway

Application example: Patent Office

Internet Banking (m-sign)

Registered E-mail (REM)

What is REM?

- REM is a service that provides its users -in addition to the ordinary e-mail services- a set of evidences suitable to uphold assertions;

  - of acceptance/rejection

  - of delivery/non delivery

  - of retrieval/non retrieval

of e-mails sent/delivered through this service.

How does REM work?

ICTA
Information and Communication
Technologies Authority

Sender

REM Service Provider – 1

REM Service Provider – 2

Recipient

2 – Authenticating the sender, security controls

4 – Signing with REM Service Provider's certificate, time stamping and delivering

5 – Verifying REM service provider's certificate, security controls

7 – Recipient's mail box

1 – Editing message, signing it, sending to REM service provider

3 – Signed acceptance receipt

8 – Delivery receipt

6 – Signed and time stamped takeover receipt

8 –E-signature is verified, e-mail is displayed

7th International Forum on the e-APP, İzmir 2012

Regulatory Framework for REM in Turkey

Turkish Trade Law No. 6102, 14 February 2011

- **Traders must use REM service for exchange of info among them over electronic medium**

- **Task of making secondary legislation on REM is given to ICTA**

Secondary Regulations for REM in Turkey

Official Journal No. 28036 and dated 25th, August 2011:

- ❑ By-Law on the Procedures and Principles Pertaining to the REM System

- ❑ Communiqué on Processes and Technical Criteria Regarding REM System

Official Journal No 28294 and dated 16 May 2012

- ❑ Communiqué on Registered E-Mail Directory and Registered E-mail Addresses

Regulations on certificates to be used by REM service providers to sign evidences (coming soon)

❑REM service providers must comply with:

- ❑ ETSI TS 102 640

- ❑ TS ISO/IEC 27001 veya ISO/IEC 27001

- ❑ BS 10012 (data protection)

- ❑ ISO/IEC 27031(business continuity for ICT)

- ❑ Web Content Accessibility Guidelines

REM Address

REMaddress@REMprovider.rem.tr

↓

Address owner

Legal Person

Natural Person

name.surname.number@spY.rem.tr

Operators
(Natural person acting on behalf of legal person)

uniquenumberforlegalperson.X@nameoflegalperson.spY.rem.tr

What is e- APP ?

❑ Under the Apostille Convention, a public document is authenticated by issuance of an Apostille (also called Apostille Certificate or Certificate) which may only be issued by a Competent Authority designated by the State from which the public document emanates.

❑ Under the e-APP, the HCCH and the NNA are, together with any interested State, developing, promoting and assisting in the implementation of low-cost, operational and secure software for:

  ❑ the issuance and use of electronic Apostilles (e-Apostilles), and

  ❑ the creation and operation of electronic Registers of Apostilles (e-Registers).

❑ The e-APP has two main components:

  ❑ Comprehensive explanatory material as to how Competent Authorities may use PDF technology and digital certificates to issue e-Apostilles, and how third parties can use such e-Apostilles; and

  ❑ Open-source software for the creation and operation of e-Registers by Competent Authorities, and an explanation as to how third parties can use such e-Registers.

7th International Forum on the e-APP, İzmir 2012

What is the goal of e-APP ?

❑ The ultimate goal of the e-APP is that,

   ❑ Competent Authorities of the majority of States that are party to the Apostille Convention will issue e-Apostilles and / or operate e-Registers of Apostilles; and

   ❑ the majority of States that are party to the Apostille Convention will accept e-Apostilles.

The advantages of the e-APP

❑ e-Apostilles signed with secure e-signature provides:

  ✓ **Integrity:** e-apostillised document has not been changed

  ✓ **Authentication:** the identity of Competent Authority can be authenticated

  ✓ **Non-repudiation:** Competent Authority cannot deny signing e-apostillised document later.

❑ E-apostillised document, can be shared throug REM system among parties with legal validity

Conclusions

- ❑ Both e-sign and REM could be applied to e-APP

- ❑ There is no obstacle to start e-APP in Turkey

- ❑ Technical and legal framework for E-sign and REM is convenient for e-APP in Turkey
  - ❑ Compliance with European Union legislations (as a candidate member state)
  - ❑ Compliance with international standards (ETSI, ISO, RFC)

- ❑ ICTA is ready for cooperation
  - ❑ CSPs could be coordinated
  - ❑ Works could be carried out to accept foreign e-certificates in Turkey

Thank you

munver@btk.gov.tr