SCREENING CHAPTER 10
INFORMATION SOCIETY AND MEDIA

AGENDA ITEM 15-16 : ELECTRONIC SIGNATURE

Country Session: The Republic of TURKEY
13-14 July 2006

Content

- Legislation
- Main Points of Turkish Electronic Signature Legislation
- Electronic Certificate Service Providers and Market
- Standardization Aspect of Electronic Signature

Legislation (I)

23 January 2004	Electronic Signature Law No.5070 was published. TA was authorised to **prepare secondary legislation** until 23 January 2005 and **inspect the market**
23 July 2004	The Law entered into force
26 August 2004	By-law on Certificate Financial Liability Insurance

Legislation (II)

6 January 2005	By-law on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law
6 January 2005	Communiqué on Processes and Technical Criteria Regarding Electronic Signatures
1 June 2006	Telecommunications Board's Decision Regarding security requirements for signature creation application and electronic signature format

Secure electronic signature

Secure Electronic Signature is a signature that;

- 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 not subsequently. (Law-Art.4)

Legal effects, recognition and admissibility of secure electronic signature

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

Secure electronic signature has the same power of proof with handwritten signature. (Law-Art.22)

Electronic data that are generated with secure electronic signatures in accordance with procedures are equivalent to bill. These data are accepted as conclusive evidence until the contrary is proved. (Law-Art.23)

Secure electronic signature shall not be applicable to legal proceedings that are subject to a special procedure or an official form pursuant to laws and warranty contracts. (Law-Art. 5)

Notification

Electronic certificate service providers shall be **public entities and establisments and natural persons or private law legal entities** that provide electronic certificates, time-stamping and other services related to electronic signatures. (Law-Art.8)

The public entities and establishments or natural persons or private law legal entities, who request to be an ECSP, **shall notify to the Authority** all the information and documents listed in Annex-1. ECSP shall indicate compliance of its notification with the requirements in detail. (By-law Art.6)

Supervision

The supervision of electronic certificate service provider's operations and transactions regarding the implementation of this Law shall be fulfilled by the TA. (Law-Art.15)

Electronic certificate service providers shall be supervised by the TA when it is necessary and at least once every two years at the TA's own initiative. (By-law Art. 22)

Foreign electronic certificates

The legal effects of electronic certificates issued by any electronic certificate service provider established in a foreign country shall be recognized by international agreements. (Law Art.14)

In case that electronic certificates issued by any electronic certificate service provider established in a foreign country are recognized by an electronic certificate service provider established in Turkey, such electronic certificates are deemed to be qualified electronic certificates. (Law Art.14 and By-law Art.32)

Electronic certificate service provider liabilities (I)

- Employing personnel qualified for the services provided
- Determining by reliable means and based on official documents,
  - the identity of the person to whom qualified electronic certificate is issued,
  - the information in case qualified electronic certificate holder's authorisation of acting on behalf of anyone
- Providing confidentiality of all operations
- Informing the applicant in written form about legal effect of the transactions (Law Art.10 and By-law Art.14)

Electronic certificate service provider liabilities (II)

- Warning and informing the certificate holder in written form not allowing third parties to use signature creation data associated with signature verification data in the certificate
- Keeping all records regarding the services provided for the period determined
- Shall not keep a copy of generated signature creation data or store it.
  (Law Art.10 and By-law Art.14)

Protection of personal data and privacy

Electronic certificate service provider;

- Shall not request any information from the applicant except the information necessary to issue an electronic certificate and shall not get such information without the consent of the applicant
- Shall not keep the certificates available in public places where third parties may have access without the consent of the electronic certificate holder
- Shall prevent the third parties to obtain the personal data without the written consent of the applicant. Electronic certificate service provider shall not pass the related information to the third parties and use them for any other purposes without the consent of the certificate holder. (Law Art.12 and By-law Art.9)

Qualified electronic certificate (I)

It is required that qualified electronic certificates shall include the followings;

- An indication that the certificate is “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 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.

(Law Art.9)

Qualified electronic certificate (II)

- The information regarding the authorisation of certificate holder if the holder acts on behalf of another person,
- When certificate holder requests, occupational and other personal information,
- Information related to conditions of the usage of 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)

Secure electronic signature creation devices

Secure electronic signature creation devices ensure that;

- Electronic signature creation data produced by those devices are unique,
- Electronic signature creation data recorded in those devices cannot be derived in any means and their secrecy is assured,
- Electronic signature creation data recorded in those devices can not be obtained or used by third parties and electronic signatures are protected against forgery,
- The data to be signed can not be altered by anyone except the signature owner and can be seen by the signature owner before the generation of signature. (Law Art.6)

Secure electronic signature verification devices (I)

- Display the data used for verification of the signature to the person who makes verification without any alteration,
- Manage the signature verification process in a reliable and accurate way, and display the results of verification to the person who makes verification without any alteration,
- Ensure that signed data is displayed in reliable manner when necessary,
  (Law Art.7)

Secure electronic signature verification devices (II)

- Display its results to the person who makes verification without any alteration detecting the authenticity and validity of the electronic certificate used for the verification of the signature in a reliable manner,
- Display the identity of the signature owner to the person who makes verification without any alteration,
- Ensure the detection of any alterations that effect the conditions relevant to the verification of the signature. (Law Art.7)

Electronic Certificate Service Providers and Market (I)

ECSP	Notification Date
E – Güven Corp.	25.03.2005
TUBITAK UEKAE Institute	31.03.2005
TurkTrust Corp.	13.05.2005
E – Tuğra Corp.	20.06.2006

Electronic Certificate Service Providers and Market (II)

4,913 qualified electronic certificates were generated by ECSPs up to 25 June 2006.

ECSPs currently negotiate with approximately 60 different parties. Depending on these negotiations, ECSPs expect to generate 22,000 qualified electronic certificates by the end of 2006.

Standardization Aspect of Electronic Signature

Operations of ECSP	ETSI TS 101 456 and CWA 14167-1
QES	ETSI TS 101 862 and ITU-T Rec. X.509 V.3
SC and V Data of Signatory	≥1024 bits for RSA or DSA or ≥160 bits for ECDSA Up to 31/12/2008
SC and V Data of ECSP	≥2048 bits for RSA or DSA or ≥256 bits for ECDSA Up to 31/12/2008
Hash Algorithm	RIPEMD – 160 or SHA – 1 or SHA-224 or SHA-256 or WHIRLPOOL
CP & CPS	IETF RFC 3647

Standardization Aspect of Electronic Signature

SSC and V Devices	CWA 14169 or assured to EAL4+ in accordance to ISO/IEC 15408 (-1,-2,-3)
Security Criteria	CWA 14167-1, ETSI TS 101 456 and ISO/IEC 17799
Time-stamp	CWA 14167-1 and ETSI TS 101 861
ECSP Certification	ISO/IEC 27001
Security Requirements for Signature Creation Applications	CWA 14170
E-Signature Format	ETSI TS 101 733 or ETSI TS 101 903

Thank you