CERTIFICATION PRACTICE STATEMENT (CPS)

VERSION : 03

DATE : 30.10.2007

1. INTRODUCTION

TÜRKTRUST Information, Communications and Information Security Services Inc. (hereinafter "TÜRKTRUST") operates in the field of electronic certificate services provision pursuant to the Electronic Signature Law no.5070 (hereinafter "the Law") dated 15 January 2004 which was promulgated in the Official Gazette dated 23 January 2004 issue 25355 and enacted on 23 July 2004, and the Regulation and the Communiqué issued pursuant to the Law by the Turkish Telecommunication Authority.

This documentation named the Certificate Practices Statement (CPS) has been prepared by TÜRKTRUST, in order to disclose how TÜRKTRUST performs its operations of certificate services provision, in conformity to the "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" pursuant to Article 7 of the "Communiqué Regarding Processes and Technical Criteria for Electronic Signature" issued by the Turkish Telecommunication Authority under the Law.

This CPS document lays down how administrative, technical and legal requirements relating to receipt of services related with certificate applications, certificate issuance and management, certificate renewal and certificate revocation procedures are complied with, and specifies the implementation responsibilities of TÜRKTRUST as the certification authority ("CA") (or, electronic certificate service provider), subscribers and relying parties.

1.1. Overview

This CPS document covers all electronic certificate services provided by TÜRKTRUST. Activities relating to qualified electronic certificates which allow the use of secure electronic signatures equivalent to hand written signatures required by laws, and secure server certificates, object signing certificates and trial certificates outside the legislation are carried out pursuant to the practice principles included in this CPS document.

The practice principles included in CPS covers all of TÜRKTRUST's practices of customer services, registration authorities and issuing certification authorities.

TÜRKTRUST certification authority conducts operational activities pursuant to this CPS which is a practice document subordinate to the relevant Certificate Policy (CP) document.

TÜRKTRUST carries out its electronic certification services provided to customers in accordance with the "TÜRKTRUST Certification Services Customer Guides" prepared in conformance to the practice principles included in CPS.

The electronic certificate services of TÜRKTRUST are executed via internal affair procedures and instructions that are prepared based on practice principles exist on CPS booklet and documented in accordance with ISO/IEC 27001 Information Security Management System together with ISO 9001 Quality Management System.

1.2. Document Name and Identification

This CPS document is named the "TÜRKTRUST Certification Practice Statement." The version number and date of the document is provided herein on the cover page.

TÜRKTRUST CPS document describes how TÜRKTRUST conducts its activities relating to certification services in accordance with the certificate policy defined in the CP document. The CPS document covers practice principles of all certificate policies laid down in CP and with object identifiers (OIDs) given below:

- TÜRKTRUST Qualified Electronic Certificate Policy (2.16.792.3.0.3.1.1.1) covers qualified electronic certificates which allow the use of secure electronic signatures equivalent to hand written signaturesof individuals pursuant to the Law, the Regulation and the Communiqué.
- TÜRKTRUST Server Certificate Policy (2.16.792.3.0.3.1.1.2) covers SSL certificates for servers.
- TÜRKTRUST Trial Certificate Policy (2.16.792.3.0.3.1.1.3) covers individual certificates for trial purposes.
- TÜRKTRUST Object Signing Certificate Policy (2.16.792.3.0.3.1.1.4) covers certificates related to object signing operations.

This CPS document is disclosed to the public at the website http://www.TÜRKTRUST.com.tr.

1.3. Participants

Participants associated with TÜRKTRUST certification services whose rights and obligations are described in this practice statement are CA units offering certification services, customers receiving the service and users.

1.3.1. Issuing Certification Authorities

Issuing certification authorities are the units of CAs responsible for issuing and distributing certificates. TÜRKTRUST's issuing certification authorities operate within a hierarchy. The primary issuing certification authority has the TÜRKTRUST root certificate. Other issuing certification authorities who have subroot certificates issued by this authority issue end user certificates.

1.3.2. Registration Authorities

Registration authorities are CA units that offer services to end users directly such as certificate application, renewal and revocation. These units establish customer records; perform identification and authentication processes and direct relevant certificate requests to issuing certification authorities.

Actions associated with registration centers may be performed by registration units within the TÜRKTRUST center in response to certificate requests arriving from TÜRKTRUST sales representatives as well as by registration centers affiliated with TÜRKTRUST. In both cases, certificate requests are relayed to the TÜRKTRUST's issuing certification authority and the certificates are issued.

1.3.3. Subscribers

Subscribers are persons for whom identification and authentication have been performed while receiving certificate applications at the TÜRKTRUST registration centers and to whom certificates have been issued and dispatched.

Natural persons who have become subscribers under the Law may use their certificates to create secure electronic signatures that have the same legal effect as hand written signatures.

Though not covered under the Law, servers for which applications have been made by a natural or legal person and certificates have been issued are also certificate users.

1.3.4. Relying Parties

Relying parties are those who receive documents signed by the private keys based on the certificates issued by TÜRKTRUST in the scope of TÜRKTRUST certification services and who verify the relevant certificates.

1.3.5. Other Participants

Since all certification services such as certificate issuing, publication of repository and similar services are provided by TÜRKTRUST in the scope of TÜRKTRUST certification services, no other participants are herein defined.

Other participants who consist of all persons and organizations which TÜRKTRUST cooperates and obtains services while offering its certification services guarantee that they shall provide the services reliably and accurately and shall not disclose confidential or private information relating to TÜRKTRUST business processes and its customers. TÜRKTRUST shall sign service contracts which explicitly stipulate such guarantees with the organizations from which it obtains services.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Usages

TÜRKTRUST's root and subroot certificates shall be used only to sign certificates in line with the purposes of use.

TÜRKTRUST's qualified certificates shall be used to create secure electronic signatures that have the same legal effect as hand written signatures. The following are all appropriate certificate usages: to sign documents and forms in e-state, e-commerce and similar practices, sign all commercial and/or official documents such as contracts and agreements in electronic medium, sign e-mail message texts, sign transaction instructions over the web, prove identity by client authentication features in network environments that require identification and authentication.

Server certificates shall be used for server authentication on servers to ensure secure communication and establish a secure communications channel.

Object Signing Certificates are used for electronically signing the software codes or software components that are zipped and packed before installation.

Trial certificates on the other hand shall be used only to sign e-mail message texts of trial purpose.

1.4.2. Prohibited Certificate Uses

TÜRKTRUST's qualified certificates may not be used in "legal actions and guarantee contracts which are subject to an official form or a special ceremony by the laws" under the Law.

In addition to this legal clause, various TÜRKTRUST certificates may not be used for purposes other than those stated in Article 1.4.1 above.

1.5. Policy Administration

TÜRKTRUST, as the authority that lays down the certificate policy, is responsible for administering and registering the CP document to which this CPS document is subordinate.

1.5.1. Organization Administering the CPS Document

All rights and responsibilities associated with this CPS document fall with TÜRKTRUST.

1.5.2. Contact Person

Contact information for this CPS document is as provided below:

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Address	: Hollanda Caddesi 62.Sokak No: 7 Yıldız, Çankaya 06550 ANKARA
Telephone	: (90-312) 439 10 00
Fax	: (90-312) 439 10 01
Call Center	: 444 0 263
E-mail	: sertifika@turktrust.com.tr
Web	: http://www.turktrust.com.tr

1.5.3. Determining CPS Suitability for the Policy

TÜRKTRUST's authorized persons determine the suitability of this CPS document with the CP document.

1.5.4. CPS Approval Procedure

This CPS document of TÜRKTRUST has been prepared in compliance with the TÜRKTRUST CP document. TÜRKTRUST's authorized persons approve this document following the examination of suitability of actions included in CPS with CP. CPS so approved shall be used to regulate and run the CA activities.

1.6. Acronyms and Definitions

1.6.1. Acronyms

CA : Certification Authority (Electronic Certification Service Provider)

CP : Certification Policy

CPS : Certification Practice Statement

CRL : Certificate Revocation Policy

IETF : Internet Engineering Task Force

OCSP : On-line Certificate Status Protokol

OID : Object Identifier

PKI : Public Key Infrastructure

RFC : Request for Comment (documents of request for comment, published by IETF as guides)

SSL : Secure Sockets Layer

1.6.2. Definitions

Activation Data: Data such as passwords, biometric values etc. used to access secure electronic signature creation devices.

Archive: Information, documents and electronic data that the CA has to keep.

Audit: All works collectively undertaken to examine the compliance of the CA's activities and operations with the relevant legislation and find out possible errors, deficiencies, corruptions and/or abuses and impose sanctions as provided by the legislation.

Certificate Financial Liability Insurance: Insurance that the CA should carry to cover the damages that would arise from its failure to perform its obligations under the Law.

Certificate Policy: A document that depicts general rules regarding the CA's functioning.

Certificate Renewal: Issuing a new certificate by using all data fields included a certificate including the public key as they are except for the term. A certificate must be valid to be renewed.

Certificate Revocation List: An electronic file that has been generated, signed and published by the CA to disclose the revoked certificates to the public.

Certificate Hash: An output of the certificate obtained via the algorithm.

Certification Authority: A public agency or institution or natural or legal persons in private law authorized by the Telecommunication Authority to provide electronic certification, time-stamping and electronic signature services.

Certification Practice Statement: A document which describes in detail how the issues included in the certificate policy shall be implemented.

Communiqué: The Communiqué Regarding Processes and Technical Criteria for Electronic Signature published by Turkish Telecommunications Authority.

Directory: An electronic storage which includes valid certificates.

Electronic Certificate: Electronic record that associates the public key and identity information of the subject.

Electronic Data: Records generated, transported or stored in electronic, optical or similar means.

Electronic Signature: Electronic data affixed to other electronic data or having logical association with electronic data and used to authenticate identification.

Institution: The Telecommunication Authority.

Institutional Application: An application for qualified electronic certificate made by a legal entity on behalf of its employees or customers or members or shareholders.

Investigation: All works collectively to determine whether notification served to the institution has met requisite conditions.

Issuing Certification Authority: A unit which is included in the CA structure, issues certificates in response to approved certificate requests, executes certificate revocations, generates, operates and publishes certification logs and certificate revocation status logs.

Key: Any of the public or private key.

Law: Electronic Signature Law no.5070 dated 15 January 2004.

On-line Certificate Status Protocol (OCSP): Standard protocol that has been created to disclose the validity status of certificates to the public, and allows receipt of certificate status information by on-line methods instantly and without interruption.

Private Key: Data such as passwords, cryptographic private keys etc. which are unique, owned and used by the subject to generate an electronic signature.

Public Key Infrastructure (PKI): The architecture, techniques, practices and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system and based on cryptographic key pairs having mathematical connection.

Public Key: Data such as passwords, cryptographic public keys etc. used to verify the electronic signature.

Qualified Electronic Certificate: An electronic certificate which is compliant with the conditions listed in Article 9 of the Law.

Registration Authority: A unit which is included in the CA structure, receives certificate applications and renewal applications, executes identification and authentication processes, approves certificate requests and directs to the issuing certification authority, has subunits that handle customer relations under the CA activities.

Regulation: The Regulation on Procedures and Principles for Implementing the Electronic Signature Law published by Turkish Telecommunications Authority.

Re-key: Issuing a new certificate by using all data fields included a certificate as they are except for the public key and the term.

Revocation Status Log: A log which includes revocation data for unexpired certificates and allows determining the exact revocation time and is accessible for third persons fast and securely.

Root Certificate: A certificate which associates the CA's institutional identity information with the CA's public key data, has been generated by the issuing certification authority, carries its signature, published by the CA to verify all certificates issued by the CA.

Secure Electronic Signature creation device: Signature creation device that has the characteristics listed in Article 6 of the Law.

Secure Electronic Signature Verification Tool: Signature verification tool that has the characteristics listed in Article 7 of the Law.

Secure Electronic Signature: An electronic signature which has the characteristics listed in Article 4 of the Law, and has the same legal effect as the manual signature for actions other than excluded by the Law.

Hashing Algorithm: An algorithm which is used to produce a fixed length summary of the electronic data to be signed.

Signature Creation device: Software or hardware tool that uses the private key to create an electronic signature.

Signature Verification Tool: Software or hardware tool that uses the public key to verify an electronic signature.

Subject: A natural person who uses a signature creation device to generate an electronic signature.

Subroot Certificate: Certificate that has been created by the issuing certification authority pursuant to the PKI hierarchy of the CA, carries the signature of the CA's root certificate and is used to sign the end user certificates.

Time Stamp Policy: A document which depicts general rules regarding the time stamping and services

Time Stamp Practice Statement: A document which describes in detail how the issues included in the time stamp policy shall be implemented.

Time Stamp: An electronic record verified by the Electronic Certification Service Provider to determine the time when an electronic datum has been generated, altered, sent, received and/or recorded.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

TÜRKTRUST is under obligation to prepare and maintain necessary documents and records concerning the certification services under electronic certification service provision. Some of these documents and records are published to the public to ensure effective provision of certification services to customers and reliability and continuity of certificate usage.

2.1. Repository

TÜRKTRUST ensures accuracy and up to dateness of all data kept in the repository. TÜRKTRUST does not employ a trusted third party (person or enterprise) to operate the repository and publish the relevant documents and records.

2.2. Publication of Certificate Information

Information in the TÜRKTRUST repository regarding the conduct of certification services are kept public except for the institutional procedures and instructions specific to the operation of the CA and confidential commercial information. The CP document which includes basic working principles of the CA, the CPS document which describes how these principles are to be implemented, subscriber agreements, practice procedures regarding certification processes are kept public in the repository. Further, all root and subroot certificates relating to TÜRKTRUST's electronic certification and time stamping services are published in directory servers and in information repository open to the public. Updated revocation status records are kept public by both OCSP support and through CRLs.

Certificates issued by TÜRKTRUST are kept public only if the subjects consent in writing.

The information referred to in this section shall be accessed at http://www.TÜRKTRUST.com.tr.

2.3. Time or Frequency of Publication

As new versions of the documents referred in Article 2.2 become available, they will be published in the repository along with their old versions. Certificate and on-line certificate status inquiry logs are constantly published. Periodical certificate revocation lists are updated at least one time per day.

2.4. Access Control on Repositories

The repository is open to the public. TÜRKTRUST takes all security measures necessary to ensure authenticity of the published information at http://www.TÜRKTRUST.com.tr.

3. IDENTIFICATION AND AUTHENTICATION

TÜRKTRUST authenticates, based on official sources together with all information in accordance with legal and technical requirements, the identification of first time certificate applicants or renewal requestors or the electronic address information of webs, e-mail and similar servers for which certificates will be issued.

3.1. Naming

3.1.1. Type of Names

All certificates issued by TÜRKTRUST use X.500 distinguished names.

3.1.2. Need for Names to be Meaningful

Names on the issued certificates are free of ambiguity and have meanings.

Name fields of qualified individual electronic certificates include the names of subscribers as they appear in their identity documents and verified through up-to-date IDs required by TÜRKTRUST. Server names authenticated by TÜRKTRUST are used in the server certificates. The corporate names are used in object signing certificates which are validated according to formal documents. For trial certificates, one-to-one match of the subscribers' names with the identity documents are not checked. Name fields of root and subroot certificates include explicitly the commercial title and relevant root information of TÜRKTRUST.

3.1.3. Anonymity or Pseudonymity of Subscribers

TÜRKTRUST does not issue qualified electronic certificates that include anonymity or pseudonymity.

3.1.4. Interpreting Various Name Forms

Names on certificates should be interpreted according to the X.500 distinguished name form.

3.1.5. Uniqueness of Names

Names on TÜRKTRUST's qualified electronic certificates are unique.

TÜRKTRUST designates at least one of the name fields by certificate type as unique to ensure uniqueness. This unique field for the qualified electronic certificates is the T.R. identity number for citizens of the Turkish Republic, while it is the passport number for foreign residents. The server name constitutes the unique field for server certificates, the fields requiring corporate information for object signing certificates and the e-mail address for trial certificates.

3.1.6. Recognition, Authentication and Role of Trademarks

TÜRKTRUST issues SSL and object signing certificates for servers that belong to companies or institutions verifying commercial title or official name.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Where a private and public key pair has not been created by the CA, a certificate applicant should prove that it holds the private key.

To prove that the certificate applicant holds the private key, the applicant should send TÜRKTRUST the electronic certificate request data signed by the applicant. Verification of the signature by the public key of the applicant demonstrates that the applicant holds the private key.

3.2.2. Authentication of Organization Identity

When issuing certificates for servers belonging to companies or institutions or for individual applicants who will obtain certificates on behalf of companies or institutions, the commercial titles of companies or the official names of institutions should be verified based on official documents.

To verify company or institution information, the company's commercial register extract and the signature circular of company's authorized persons are required.

3.2.3. Authentication of Individual Identity

Personal information for persons applying for qualified electronic certificates should be verified in the way stated in the laws and based on official documents. When receiving the applications for qualified electronic certificates, authentication shall be made face to face at the first application pursuant to the law.

For applications for trial certificates, a valid e-mail address and a personal statement suffice.

To verify personal identity in applications for qualified electronic certificates, the originals of one of the official identity documents such as an identity certificate, a driver's license or a passport shall be shown and photocopies furnished. TÜRKTRUST shall confirm that the copies conform to the originals.

In institutional applications for the employees of an institution, personal information for persons to be included in the certificate shall be verified in the way stated in the laws and based on official documents. When receiving applications for qualified electronic certificates, authentication shall be made face to face at the first application pursuant to the law. Further in institutional applications, the commercial register extract and other relevant documents shall be required to determine the legal personality of the institution.

The e-mail addresses of people applied for qualified electronic signature are taken from personal declarations from the application form. To verify those addresses before to be added to the certificate, a unique (URL) link specific to the application is sent to the correspondent enclosed in an e-mail message. The e-mail address is verified by clicking to this URL and e-mail address can be added to the target certificate after that.

3.2.4. Non-verified Subscriber Information

Personal information and communication information other than personal and institutional information of the applicants which are included in the identity documents or other formal documents, indicate their institutional authorities and included in the certificate shall be accepted upon statement and not verified through a third source. Communication details like address, telephone number, e-mail and other information like corporate unit, corporate title are taken with signed declaration as well.

3.2.5. Validation of Authority

If a certificate applicant requests that such information as his professional title, company of affiliation, title in the company and authorization of use should be affixed to his certificate, such information should be verified by official documents from the relevant sources.

3.2.6. Criteria for Interoperation

Qualified electronic certificates issued by TÜRKTRUST interoperate with all other qualified electronic certificates. Certificates may be confirmed mutually over appropriate client software.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

The realization of the new key production at the end of the secure usage period of the key pair starts with a new qualified electronic certificate application completed by the user. In such case, if the key pair is generated by the subject, the public key shall be transmitted to the CA along with the certificate request.

In re-key applications of the existant certificate users , some of the still valid official documents required in the first application to authenticate identity may not be required other than a signed statement of the user form and commitment of the applicant. The face-to-face operation completeness for authentication is not required unless special situations.

3.3.2. Identification and Authentication for Re-key after Revocation

For a re-key application after revocation, some of the still valid official documents required in the first application to authenticate identity may not be required other than a signed statement of the user form and commitment of the applicant. The face-to-face operation completeness for authentication is not required unless special situations..

3.4. Identification and Authentication for Revocation Request

TÜRKTRUST receives certificate revocation requests through secure means; verifies the identity of the person either from signed revocation statement or checking the information through web or telephone who makes the revocation request leaving no trace of doubt.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

TÜRKTRUST generates root and subroot certificates of its own issuing certification authorities, certificates of registration authorities that will serve as registration centers, and end-user certificates in accordance with practice principles included in this CPS document and carries out administration actions. Practices are different for life cycles of personal and server certificates and those of qualified certificates and personal certificates of trial purposes. Following sections describe how shared and different actions have been carried out for these different certificate types.

Root and subroot certificates of TÜRKTRUST's issuing certification authorities are generated at the TÜRKTRUST's issuing certification authority upon receipt of public keys corresponding to private keys generated in its secure electronic signature creation devices.

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application?

The following may apply for a certificate to TÜRKTRUST:

- Natural persons who wish to obtain qualified electronic certificates or trial certificates,
- Companies or enterprises which wish to obtain certificates on behalf of their employees provided that personal application documents exist,
- Server administrators or authorized technical persons who will use qualified electronic certificates for servers or object signing certificates of the registration authorities which will serve as TÜRKTRUST's registration authorities.

Applications by the authorized persons of registration authorities which serve as TÜRKTRUST's registration authorities or TÜRKTRUST's in-house personnel are processed according to the same principles as for other qualified electronic certificate applications. Applications for server certificates via the server administrators are processed according to the same principles as for other server certificate applications. However, TÜRKTRUST shall further sign service contracts with registration authorities which may be required of additional information or documents in certificate applications pursuant to such contracts.

4.1.2. Enrollment Process and Responsibilities

For an application for a qualified electronic certificate, the applicant should fill in the application form completely, sign manually, and transmit the required identity authentication documents and a signed subscriber's agreement along with the application form to the TÜRKTRUST center or registration authorities. While an application to a registration center can be made directly by the applicant, for institutional applications, relevant forms and documents can be prepared on site by way of TÜRKTRUST's sales representatives, as well.

A public key required for a qualified electronic certificate application is generated simultaneously with the private key. Depending on the TÜRKTRUST certificate application process, it is possible that the private and public key pair may be generated at the TÜRKTRUST center, by the requestor himself at registration authorities or at any other premises.

For a server certificate application, the server administrator should fill in the relevant form and procure the required documents and transmit them along with a server certificate agreement to TÜRKTRUST.

For an object signing certificate application, the technical representative should fill in the relevant form and procure the required documents and transmit them along with a server certificate agreement to TÜRKTRUST.

An application for a trial certificate shall be made over the web without identity authentication.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

When processing a qualified electronic certificate application, the identification of the applicant shall be authenticated based on official documents pursuant to the laws. If the person is obtaining the certificate based on any capacity such as representation, agency or similar representing or power of attorney relationship, such relationship between the company and the applicant shall be officially verified. At the first application, the authentication action shall be made face to face at TÜRKTRUST's registration authorities or by sales representatives. This may not be required in subsequent applications.

When processing a server certificate application, the domain name that belongs to the server, the server's name and the name of the domain owner and personal information for the server administrator should be verified by TÜRKTRUST's registration authorities. The information published by authorized resources are used for the verification of the domain name ownership. (www.nic.tr records for domain names with ".tr" extension, international resources are based on for other domain names)

No authentication shall be made when processing applications for trial certificates.

4.2.2. Approval or Rejection of Certificate Applications

Following identity authentication and document checks done by TÜRKTRUST registration authorities, if the certificate application by certificate type is compliant with this CPS and certificate application procedures, it shall be approved. Otherwise the application shall be rejected and the same application steps should be repeated to obtain a certificate.

4.2.3. Time to Process Certificate Applications

Maximum time is 10 (ten) business days for processing qualified electronic certificate applications that arrived at TÜRKTRUST registration authorities and rejecting the application or issuing the generated certificates.

This term shall commence upon the arrival of a certificate application at the TÜRKTRUST center.

In the case of a private key is generated by TÜRKTRUST and loaded on the signature creation device, the certificate is published within this term while at the same time the signature creation device is delivered to the courier. The password envelope for the signature creation device shall be given to the courier separately and later than the smart card, as well.

Time required for processing server or object signing certificate applications and issuing certificates is 5 (five) business days following the arrival of server certificate application in electronic medium to the TÜRKTRUST center.

Time for processing trial certificate applications is maximum 1 (one) business day for no authentication is required.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

Institutional applications for electronic certificates relayed by sales representatives to TÜRKTRUST registration authorities and qualified electronic certificates sent to TÜRKTRUST after prepared personally shall be checked according to the procedures. Where any error or deficiency is found out in the applications, customer relations authorized personnel contact the applicants and ensure that errors or deficiencies are remedied. Approved applications shall be recorded and processed in the TÜRKTRUST's issuing certification authority and certificates shall be issued.

Registration procedures for applications for qualified electronic certificates transmitted by the registration authorities may be completed at the registration authorities or through online web services. In such case too, relevant forms and documents with application shall be transmitted to TÜRKTRUST and certificates shall be issued.

Subroot certificates for the issuing certification authorities that operate under TÜRKTRUST shall be issued within the relevant procedures.

Server certificates and object signing certificates shall be issued pursuant to the procedures.

Applications for trial certificates shall be automatically processed on the system and certificates shall be issued and published.

The term for qualified electronic certificates, server certificates and object signing certificates issued by TÜRKTRUST is 1 (one), 2 (two) or 3(three) year(s), and for trial certificates 3 months.

Qualified electronic certificates issued by TÜRKTRUST comply with ITU-TRec.X.509V.3 and other standards specified in the Communiqué.

4.3.2. Notification to Subscriber of Issuance of Certificate

After certificate issuing is completed, the subjects of qualified electronic certificates shall be informed by e-mail.

Upon issuing server certificates, server administrators are informed by e-mail, technical responsibles for object signing certificates ; so are subjects of trial certificates similarly upon issuing their certificates.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

For qualified electronic certificates, no acceptance of a certificate's content shall be sought. Subjects are under obligation to notify TÜRKTRUST and request revocation of certificates which happen to include data that are at variance with applications or inaccurate.

No acceptance shall be sought of a certificate's content for server or object signing certificates either. Server administrators for server certificates or technical responsibles for object signing certificates are under obligation to notify TÜRKTRUST and request revocation of certificates which happen to include data that are at variance with applications or inaccurate.

No acceptance ceremony exists for trial certificates.

4.4.2. Publication of the Certificate by the CA

Qualified electronic certificates shall be published in the web and/or directory servers provided that subjects consent in writing.

Server certificates, object signing certificates and trial certificates shall be kept accessible to the public pursuant to the relevant procedures.

4.4.3. Notification of Certificate Issuance to Other Entities

Not applicable.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subjects should use their private keys and certificates in accordance with the Law, the Regulation and other regulatory actions, and stipulations indicated in the CP and CPS documents and the relevant subscriber’s letter of undertaking. A subscriber’s letter of undertaking lays down how and for what purposes the relevant certificate by type shall be used, and the responsibilities of the subscriber for ensuring security of the private key and using the secure electronic signature creation device.

The following general conditions should be met by certificate type:

For a qualified electronic certificate, the subject should:

- Receive in person the secure electronic signature creation device and the relevant activation data issued to his name.
- Where he personally generated the private and public keys at the certificate application, should perform the action securely and in accordance with the relevant legislation. He should transmit the correct public key to the CA under the rules depicted in this CPS.
- Protect the private key, the secure electronic signature creation device and relevant passwords against loss, disclosure, alteration and access and use by third persons.
- Ensure that all personal information he has disclosed at the certificate application and throughout the term of the certificate should be complete and correct. He should immediately transmit to the CA any changes in the information he has disclosed at the application and throughout the term of the certificate.
- Where the private key and/or the signature creation device is lost, disclosed, altered or used by other persons or any circumstance that may lead to such occurrence arises, should immediately inform the CA with a view to certificate revocation.
- Fulfill his obligations laid down in the principles and rules stated included the CP and CPS documents and in the guides.
- Should not use his electronic certificate, signature creation device and private key for purposes other than those stated in the CP and CPS documents and the subscriber’s letter of undertaking.

For a server certificate and an object signing certificate:

- The private and public keys should be generated securely by the server administrator or technical responsible, and the public key should be transmitted to the CA under the circumstances stated in this CPS.

- Necessary measures should be taken against displacement, by other persons without authorization and permission, of the server for which the certificate has been issued and of all passwords and keys associated with the server certificate or the object signing certificate.
- Necessary measures should be taken against loss, disclosure, alteration and use by other persons of the server for which the certificate has been issued, the entirety of relevant software and of all passwords and keys associated with the server certificate or the object signing certificate.
- The server certificate should be used for one device only and this device should be provided physical security.
- Information disclosed at the certificate application should be complete and correct. Any changes in the disclosed information at the certificate application and throughout the term of the certificate should be immediately notified to TÜRKTRUST.
- Where any loss, disclosure, alteration and use by unauthorized persons of the server for which the certificate has been issued, the entirety of relevant software and of all passwords and keys associated with the server certificate or the object signing certificate does occur, TÜRKTRUST should be immediately notified with a view to certificate revocation.
- Where the certificate expires or is revoked, it should be deleted from the server where it has been installed and not be used any more for any purpose.
- Obligations laid down in the guides and rules stated included the CP and CPS documents and in the procedures should be fulfilled.
- The server certificate or the object signing certificate and the private key should not be used for purposes other than those stated in the CP and CPS documents and the subscriber's letter of undertaking.

Authorized persons of the registration authority should fulfill in accordance with the principles above their responsibilities regarding the qualified electronic certificates and server certificates they hold.

Subjects of trial certificates should not use their certificates for any purpose other than trial.

4.5.2. Relying Person Public Key and Certificate Usage

Relying persons are under obligation to check the validity of certificates on which they rely and use the certificates within the usage purposes stated in the Law, the Regulation and other regulatory actions, and the CP and CPS documents.

4.6. Certificate Renewal

1 (one) year qualified electronic certificates issued by TÜRKTRUST should be renewed in order to continue to be used at the expiry under same circumstances.

Certificate renewal is made where there is no change in the certificate information at the expiry of the certificate. In this case, a new key pair is not generated, but a new certificate which is dependent on the same public key and has a renewed date shall be issued and dispatched to the subject.

Expired certificates cannot be renewed; a new certificate application and a new issuing shall be required pursuant to the practice principles indicated in Article 4.1 to 4.5. In the same manner, there is no way of renewal possibility without new key pair production for 2 (two) and 3 (three) years TÜRKTRUST qualified electronic certificates. To continue usage for such certificates at the end of expiry period; a new certificate application and a new issuing shall be required pursuant to the practice principles indicated in Article 4.1 to 4.5.

Renewal shall not be made for root and subroot certificates without renewing the key pair.

Server certificates and object signing certificates shall not be renewed; a new certificate shall be issued against a new certificate application.

Where a certificate has to be renewed due to a change in the conditions of TÜRKTRUST electronic certification services or a similar reason, TÜRKTRUST shall inform the subject by e-mail, telephone or fax in accordance with the TÜRKTRUST Electronic Certificate Subscriber's Agreement.

Renewal process is not applicable for trial certificates.

4.6.1. Circumstances for Certificate Renewal

A certificate shall be renewed upon the request of the subject where certain time remains to the expiry and no changes occur in the information included in the certificate.

4.6.2. Who May Request Renewal

Subjects of 1 (one) year qualified electronic certificates may request renewal.

4.6.3. Processing Certificate Renewal Requests

A certificate renewal request shall be processed in different ways depending on the certificate type.

For 1 (one) year qualified electronic certificates, an application for certificate renewal may be made over the web by electronic signature via the existing private key in electronic medium or signature on paper.

Since the key pair does not change in a standard certificate renewal, the secure signature creation device on which the private key is located for qualified electronic certificates shall not change.

4.6.4. Notification of Renewed Certificate Issuance to Subscriber

For qualified electronic certificates, when the new certificate is issued, the subject shall be informed by e-mail. During the renewal process, the old certificate may be used till the expiry of its term.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

For qualified electronic certificates, no acceptance of a renewed certificate's content shall be sought. Subjects are under obligation to notify TÜRKTRUST and request revocation of certificates which happen to include data that are at variance with applications or inaccurate.

No acceptance ceremony exists for trial certificates.

4.6.6. Publication of the Renewal Certificate by the CA

Renewed qualified electronic certificates shall be published in the web and/or directory servers provided that subjects consent in writing.

Renewed trial certificates shall be kept accessible to the public pursuant to the relevant procedures.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7. Certificate Re-key

For end user certificates, the same private and public key pay may be used for up to a maximum of 3 (three) years. At the end of such a term, instead of re-keying action it is possible to continue certificate usage with a new certificate and new key pair according to first time application steps.

A new certificate application and a new issuing with a new key pair shall be required pursuant to the practice principles indicated in Article 4.1 to 4.5 when the 3 (three) years secure usage expiry period for public/private key pair gets over for 1 (year) qualified electronic certificates, or at the expiry date for 2 (two) and 3 (three) years qualified electronic certificates, or at the expiry date for all server and object signing certificates, or at the end date for trial certificates.

The certificate information can be updated, the information forming the certificate content can be modified with the corresponding suitable documents for the new certificate applications where re-keying takes place other than certificate renewal.

Where the expiry of a root certificate draws closer, the term of an end user certificate to be issued shall be designated not to go beyond the expiry of any of the associated root certificates. For the period when the term of the old root certificate and that of the renewed root certificate overlaps, TÜRKTRUST makes a cross-certification for these two root certificates so that certificates issued based on both roots may be used smoothly; and such cross-certification shall be appropriately notified to subjects and relying people.

4.7.1. Circumstances for Certificate Re-key

Not applicable.

4.7.2. Who May Request Certificate Re-keying

Not applicable.

4.7.3. Processing Certificate Re-keying Requests

Not applicable.

4.7.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

Not applicable.

4.7.6. Publication of the Re-keyed Certificate by the CA

Not applicable.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8. Certificate Modification

Where there occurs any change in the information included in a certificate issued by TÜRKTRUST, such certificate shall be revoked and an application shall be filed for a new certificate with new information. No modifications may be made on the existing certificate by any other method.

A new certificate application and a new issuing shall be made pursuant to the principles indicated in Article 4.1 to 4.5.

Where a certificate has to modified due to a change in the conditions of TÜRKTRUST electronic certification services or a similar reason, TÜRKTRUST shall inform the subject by e-mail, telephone or fax in accordance with the TÜRKTRUST Electronic Certificate Subscriber's Agreement.

4.8.1. Circumstances for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not applicable.

4.8.3. Processing Certificate Modification Requests

Not applicable.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6. Publication of the Modified Certificate by the CA

Not applicable.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstance for Revocation

Where a certificate loses its validity within the term of use, it shall be revoked. The following circumstances shall require revocation of a certificate:

- Request by the subject,
- It is understood that the information regarding a qualified electronic certificate held at TÜRKTRUST is false or incorrect,
- A change occurs in the information regarding the subject included in a certificate's content
- It is learned that the subject's legal capacity is restricted, or the subject is bankrupt or lost in danger of death, or died,
- The private key has been lost, stolen, disclosed or a risk of access or use by a third party arises,
- The secure electronic signature creation device in which the private key is located has been lost, broken down or compromised,

- It is understood that the certificate has been used in contradiction to the provisions of the CP and CPS documents and TÜRKTRUST Certificate Subscriber's Agreement,
- TÜRKTRUST suspends provision of certification services.

Revoked certificates are published via CRL and OCSP services until the end of term.

4.9.2. Who Can Request Revocation

The following people may request revocation:

- The subject himself, for personal certificates,
- The server administrator, for server certificates,
- The technical responsible, for object signing certificates,
- An authorized person of an company or institution to which the subject or server is associated, for certificates in institutional use,
- TÜRKTRUST's authorized persons (TÜRKTRUST center and registration authorities) for end user certificates and root and subroot certificates where security concerns necessitate.

4.9.3. Procedure for Revocation Request

Revocation requests shall be received in different ways, namely, over the declarative statement or by telephone via TÜRKTRUST web site, from the.certificate owners.

The subject chooses the certificate to be revoked from TÜRKTRUST web site logged in with interactive password. Online certificate revocation process is completed by entering the revocation reason after a secondary authentication stage.

Alternatively, the subject may access the TÜRKTRUST Call Center on telephone and transmit his revocation request either by the automatic call receiver program or the call center operator during the working hours. To approve a revocation request, the requestor shall be required to fulfill a series of control mechanisms. After passing the secondary authentication stage, the reason for certificate revocation shall be entered and thus the revocation action shall be completed.

Besides, the subject may access the TÜRKTRUST with a hand written certificate revocation request signed manually as an optional choice. The original copy of the request is checked by TÜRKTRUST authorized personnel and revocation process completed. If the hand written request delivered via fax, certificate status changed to on hold till the original copy of the request is checked by TÜRKTRUST authorized personnel.

The revocation status after the action shall be notified by e-mail to the subject.

Revocation requests for institutional certificates may be obtained from the subjects as well as from the authorized persons of companies along the approved revocation applications. After the certificate revocation request is confirmed with a hand written paper coming from the authorized person of the firm, the act of revocation is completed. The revocation status after the action shall be notified by e-mail to the firm or institutional authorized personnel.

Revocation requests for trial certificates is not applicable.

Revocation requests for server and object signing certificates are taken only with a hand written paper. To revoke a server or an object signing certificate for a firm or an institution, revocation request form should be provided confirmed by server administrator and technical responsible as well as authorized personnel of the firm. The revocation status after the action shall be notified by e-mail to the firm or institutional authorized personnel.

Where a security compromise occurs at TÜRKTRUST, or a notice is received regarding the existing certificates or a fault is detected in TÜRKTRUST's internal operation, TÜRKTRUST may initiate certificate revocation. A certificate revocation process initiated by TÜRKTRUST may originate from registration authorities or issuing certification authorities.

For all certificate revocations originating from TÜRKTRUST, the outcome shall be notified by e-mail to certificate users. New certificate issuing operations shall be immediately started, where necessary, after the revocation.

TÜRKTRUST provides certificate revocation services without interruption 7 days 24 hours through web. Revocation requests coming to the TÜRKTRUST Call Center via telephone or hand written paper are processed during working hours.

Where root and subroot certificates of TÜRKTRUST are revoked, the status shall be notified in electronic medium to all relevant parties urgently in the shortest possible time. End user certificates that have the signature of the revoked root or subroot certificates shall also be revoked and users shall be notified by e-mail.

4.9.4. Revocation Request Grace Period

Not applicable.

4.9.5. Time within Which TÜRKTRUST Must Process the Revocation Request

TÜRKTRUST immediately resolves all certificate revocation requests online transmitted over the web or by telephone following the approval of the request and authentication of identity. Revocation requests transmitted on paper or on telephone via call center shall be taken into evaluation in the shortest time possible during working hours and necessary actions shall be completed urgently.

4.9.6. Revocation Checking Requirements for Relying People

Relying people are under obligation to verify the relevant certificate to rely on an electronic signature transmitted. To verify a certificate's status, updated CRLs published by TÜRKTRUST or OCSP, the on-line certificate status inquiry service, should be used. TÜRKTRUST recommends that relying people should use secure electronic signature verification tools specified in the Communiqué when verifying electronic signatures.

4.9.7. Certificate Revocation Lists (CRL) Issuance Frequency

TÜRKTRUST issues a new CRL at least once a day even if there is no change in the status of end user certificates.

The CRL's for TÜRKTRUST root certificates are issued at least once a year even though there is no certificate revocation or sub-root revocation.

4.9.8. Maximum Latency for CRLs

CRLs are issued within at most 10 (ten) minutes after generation.

4.9.9. On-line Revocation/Status Checking Availability (OCSP)

TÜRKTRUST provides uninterrupted on-line certificate status protocol OCSP support. By this OCSP service which is a real time certificate status inquiry and more reliable than CRLs, customers may inquire the status of certificates on-line by appropriate software on the customer side. It is possible by this inquiry to obtain information on the status of a certificate any time (valid, suspended, revoked, expired/unknown).

4.9.10. On-line Revocation/Status Checking Requirements

It is recommended that relying people when inquiring the status of certificates should prefer OCSP if their technical capabilities allow, or opt for CRL as a second alternative.

4.9.11. Other Forms of Revocation Advertisements Available

TÜRKTRUST does not employ any method other than OCSP and CRL for advertising revocation status.

4.9.12. Special Requirements regarding Key Compromise

Where a security compromise occurs at TÜRKTRUST, end user certificates affected by the incident shall be revoked by TÜRKTRUST. If the root or subroot certificates of TÜRKTRUST need to be revoked, end user certificates that have the signature of such certificates shall also be revoked and users shall be informed by e-mail.

The compromise incident and its effects shall be advertised by TÜRKTRUST to subscribers and relying people urgently over the public website and where necessary via the press media.

TÜRKTRUST is responsible for starting to issue new certificates after revocation in cases of all certificate revocations originating from TÜRKTRUST.

4.9.13. Circumstances for Suspension

Where the source of a certificate revocation request could not be verified, TÜRKTRUST shall suspend, rather than revoke, the certificate in question until the verification is finalized, or upon a request where the end user is unsure whether any circumstance that requires revocation does exist.

4.9.14. Who Can Request Suspension

All the following participants which may request revocation may also request suspension:

- The subject himself, for personal certificates,
- The server administrator, for server certificates,
- The technical responsible, for object signing certificates,
- An authorized person of an company or institution to which the subject or server is associated, for certificates in institutional use,
- TÜRKTRUST's authorized persons (TÜRKTRUST center and registration authorities) for end user certificates and root and subroot certificates where security concerns necessitate.

4.9.15. Procedure for Certificate Suspension

Certificate suspension requests shall be transmitted to TÜRKTRUST in the same way as certificate revocation requests stated in Article 4.9.3, over the web or by telephone or by paper, from the subject or the server administrator or the technical responsible. Following the completion of the relevant steps, the certificate shall be suspended by the CA. The suspension status shall be notified by e-mail to the subject or the server administrator or the technical responsible.

Suspension requests for institutional certificates may be obtained from the subjects as well as from the authorized persons of companies along the approved suspension applications. The suspension status after the action shall be notified by e-mail to the authorized person of the company or institution, the subject or the server administrator or the technical responsible.

Suspension requests for trial certificates is not applicable.

Where a security compromise occurs at TÜRKTRUST, or a notice is received regarding the existing certificates, TÜRKTRUST may suspend relevant certificates. A certificate suspension process initiated by TÜRKTRUST may originate from registration authorities or issuing certification authorities. For all certificate suspensions originating from TÜRKTRUST, the outcome shall be notified by e-mail to certificate users.

TÜRKTRUST's root and subroot certificates shall not be suspended.

4.9.16. Limits on Suspension Period

Certificates suspended by TÜRKTRUST, where the source of a certificate revocation request could not be verified, shall remain suspended until the finalization of verification or the period is over. Certificates suspended where the subjects are unsure whether any circumstance that requires revocation does exist shall be revoked when the subjects approve the necessity for revocation.

In both cases, the duration of suspension may not exceed 30 (thirty) days. Those still in suspension at the end of this period shall be automatically revoked for security reasons.

Where it is understood while certificates are suspension that there is no circumstance that requires revocation, such certificates may be taken out of suspension and moved into the valid status.

4.10. Certificate Status Services

Certificates issued by TÜRKTRUST shall be published over the web accessible to all subjects and relying people provided that subjects consent in writing. Certificates may be published in a manner accessible directly at the web and/or a LDAP directory server.

Certificate status inquiries shall be made by two different methods: Certificate Revocation List (CRL) and On-line Certificate Status Protocol (OCSP).

4.10.1. Operational Characteristics

TÜRKTRUST issues a new CRL at least once a day even if there is no change in the status of certificates.

TÜRKTRUST provides on-line certificate status protocol OCSP support. It is possible by this inquiry to obtain real time information on the status of a certificate any time (valid, suspended, revoked, expired/unknown).

4.10.2. Service Availability

TÜRKTRUST provides CRL and OCSP services under conditions stated in Article 4.10.1 without interruption 7 days 24 hours. TÜRKTRUST uses backup systems to prevent interruption of OCSP service.

4.10.3. Optional Features

Not applicable.

4.11. End of Subscription

Subscription ends upon the expiry of the term of a certificate or the revocation of a certificate.

4.12. Key Escrow and Recovery

TÜRKTRUST does absolutely not store or re-generate private keys of end user certificates it has issued for electronic signature purposes, or hold data that it could re-generate.

4.12.1. Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

This section of the CPS document covers non-technical security controls that TÜRKTRUST practices to ensure facility and operation safety when performing certification services.

5.1. Physical Controls

5.1.1. Site Location and Construction

The TÜRKTRUST center has been established on secure premises protected against external threats, and high-security areas and various security areas have been designated within the facility.

5.1.2. Physical Access

Physical access to areas within the TÜRKTRUST center is constantly controlled.

The perimeter of the facility has been surrounded by protection to prevent uncontrolled access or exit. Security personnel man all entry-exit points to the center. Physical access to secure areas is allowed via the pass card entry control system. Unauthorized persons are prohibited to enter certain areas. High-security areas where basic certificate generation is carried out are always closed to unauthorized access. Entries and exits are logged. As an additional security measure, critical areas and passes are monitored by cameras and daily recording of cameras is kept for security reasons.

5.1.3. Power and Air Conditioning

Uninterrupted power supplies have been installed to operate all hardware and equipment used at the TÜRKTRUST center. Systems are supported by uninterrupted power supplies and generators which will immediately be enabled in cases of power interruption. Maintenance for standby power units is regularly performed and their capacities are developed according to requirements.

Particularly in areas where computer hardware is concentrated, adequate and uninterrupted ventilation is provided. Appropriate heating and cooling systems are used and temperature and humidity are kept under control to ensure optimal climatic conditions inside the building.

5.1.4. Water Exposures

The TÜRKTRUST center is protected against floods and water exposures due to natural disasters by way of construction measures. The outer surface and ground layer of the building are water-tight. Necessary insulation has been provided to prevent the underground water leaking into the building.

To prevent internal water exposures that may occur due to failures in the water and sewage system, the plumbing has been built appropriately, and the water flow inside the building is taken under control by passing the water channels through main plumbing routes. No water or sewage routes pass through the sections and areas where critical hardware and equipment are located.

Adequate water discharge systems have been installed to dispose of water floods which might occur despite all construction measures without damaging the existing system.

5.1.5. Fire Prevention and Protection

An appropriate lightning arrestor system has been installed to prevent fires due to lighting in the TÜRKTRUST building. To prevent fires that may originate from electrical contacts, high quality appropriate materials have been used for the electrical installation, and electrical fuses of adequate rating have been installed in power systems. Open flames are not used in areas other than the kitchen and certain limited and designated areas; and the rule of no smoking is strictly enforced outside the designated areas.

Smoke and heat detectors have been installed at appropriate locations in the facility to detect probable fires and prevent them from spreading. An embedded fire extinguishing system exists which will activate automatically in case of a fire alarm. This embedded system utilizes different physical and chemical fire extinguishing materials depending on various areas of the building. In addition, fire extinguishing units of appropriate chemical and physical characteristics have been place at appropriate locations in the building, and the staff has been trained in fire intervention at critical equipment and areas.

5.1.6. Media Storage

Backups of all records generated during the activities of TÜRKTRUST are kept in appropriate storage media. Such backups are stored in a fire and water protected area inside the building where all physical and electromagnetic security precautions are taken, access is secured and provided through only by procedural controls.

5.1.7. Waste Disposal

All information and documents relating to basic certification services stored in electronic or paper medium shall be destroyed and disposed of pursuant to relevant procedures if they need not be stored. Cryptographic modules, when should be disposed of, shall either disposed of by physical destruction or reset according to the manufacturer’s instructions.

All other waste of the building and TÜRKTRUST units shall be removed appropriately out of the facility.

5.1.8. Off-site Backup

TÜRKTRUST, to ensure business continuity of certification services, keeps the backups of electronic records in secure safes off-site in order to re-start operation of its systems in case of a disaster that may occur to the existing facilities and the building.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles have been designated to perform all electronic certification business processes to organize the employees of TÜRKTRUST :

- **High Level Managers:** Senior managers technically and administratively responsible for conduct of TÜRKTRUST’s certification services as planned.
- **Unit Managers:** Managers responsible for planning, managing and controlling technical and administrative functioning of relevant units where customer services and basic certification processes as well as all support functions such as archival and facility security are carried out.
- **Auhorized Personnel for Registration and Customer Services:** Unit staff responsible for routine certification services such as customer services, document

control, registration processes relating to certificate application, renewal and revocation.

- **Information Security Management System Personnel:** Responsible for ensuring information security in business processes under TÜRKTRUST's certification services, execution of security principles and related procedures and continuity of the certified ISO/IEC 27001 information security management system.
- **System and Network Administrators:** Employees responsible for installing, configuring, backing up and ensuring continuity of all software and hardware components used in certification processes.
- **Certificate Production Center Officers**: Responsible for daily certificate production facilities having special access control privileges. Backing up and reloading are also included their duty instructions.
- **System Auditors**: Responsible for auditing certificate production facilities and all related documents.
- **Security Personnel:** Serving as security personnel at the building entry and critical units who are responsible of physical security of the entire TÜRKTRUST facilities.

5.2.2. Number of Persons Required per Task

A multi-person controlled system has been established at TÜRKTRUST to perform critical operations in certification processes. Certificate and CRL generation activities which require use of cryptographic modules can be made by at least two authorized persons present.

In addition to the routine certificate generation steps stated above, all generation, renewal and revocation operations relating to TÜRKTRUST root and subroot certificates can be performed by at least two authorized persons present and upon the issuance of approved duty instructions to the relevant authorized persons.

5.2.3. Identification and Authentication for Each Role

Employees appointed to trusted roles within TÜRKTRUST shall be first identified to the security system with their designated authorities first. Thus, authentication shall be performed for persons in such roles prior to each critical operation. After the authentication is successfully completed, the operation is allowed, and logged after completion.

5.2.4. Roles Requiring Separation of Duties

While the certification process is operated, the entirety of sequential operations made on the same certificate shall be performed by different persons at different process points. Duties have been distributed to separate roles and thereby a single person is prevented from performing the entirety or a large part of the work in the process. Each operation is logged so as to include detailed place and time data based on roles.

5.3. Personnel Controls

5.3.1. Qualifications, Experience and Clearance Requirements

Personnel employed at TÜRKTRUST have appropriate educational levels (high school, baccalaureate degree, master's degree etc.) with qualifications to perform certification processes accurately and reliably, are knowledgeable and trained in their fields, have experience in similar works and have passed security checks.

5.3.2. Background Check Procedures

TÜRKTRUST assesses in detail personal backgrounds and references of personnel employed at TÜRKTRUST, and makes sure that they are technically and administratively suitable. Criminal records certificate shall be required of personnel found to be suitable and security investigation shall be conducted as necessary.

5.3.3. Training Requirements

TÜRKTRUST's personnel undergo training for their responsibilities prior to commencing their works. Employees shall be trained and informed in detail, throughout the training period, on basic certification business processes, customer services, procedures and instructions relating to operation of registration authorities and issuing certification authorities, information security principles and the existing information security management system, and units of software and hardware employed.

Employees working at registration authorities undergo training to the extent required for their duty roles.

5.3.4. Retraining Frequency and Requirements

Training provided to employees shall be repeated periodically and as necessary after the initial training prior to commencing work. In light of results of continuous assessment and evaluation studies, personnel's training needs shall be identified and additional training sessions may be organized to increase work efficiency in addition to the periodical training. The topics and scope of training provided shall be continuously updated and refreshed in accordance with the advancing technology and renewed software and hardware units.

5.3.5. Job Rotation Frequency and Sequence

TÜRKTRUST's security personnel and operators shall be subjected to rotation in sub-duties within their field of work. However, no rotations shall be made between fields of work.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary actions shall be imposed pursuant to TÜRKTRUST's human resources instructions on those TÜRKTRUST personnel who attempt unauthorized actions. If TÜRKTRUST or customers of TÜRKTRUST suffer damages due to such unauthorized action, this damage shall be recovered from the relevant employee.

TÜRKTRUST further refers those who commit unauthorized actions to judicial authorities to ensure institution of proceedings against them pursuant to the Law, the Regulation and the Communiqué.

5.3.7. Independent Contractor Requirements

For operations carried out by way of subcontractors within certification processes, TÜRKTRUST signs a service contract with the contractor company. This service contract stipulates the security clauses and service principles required by TÜRKTRUST.

5.3.8. Documentation Supplied to Personnel

TÜRKTRUST's personnel are supplied with the CP and CPS documents, practice and security procedures relating to certification processes, job instructions arranged to specific roles of employees, user's guides of software and hardware.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

Records relating to all certification services within the certification life cycle shall be kept by TÜRKTRUST. Included among such records are certificate application records, all records of customer requests relating to issued, renewed, suspended and revoked, records relating to issued and published certificates and CRLs, operational records of TÜRKTRUST units having trusted roles, employees' entry and exit records to/from TÜRKTRUST and their accesses to system modules, records relating to document monitoring, software and hardware installation, updating and repair records.

When logging operations, the description of an operation, the person who performed the operation, and date and time of the operation shall basically be logged.

5.4.2. Frequency of Processing Log

Audit records are logged continuously and, backed up and archived periodically.

5.4.3. Retention Period for Audit Log

Audit logs for TÜRKTRUST's operations shall be retained in the system for one year. Upon expiry of this period, they will be archived pursuant to the legislation.

5.4.4. Protection of Audit Log

Audit logs are protected by physical and electronic security measures, and kept open for access by authorized personnel only. The data integrity of audit logs is ensured by keyed hashing method.

5.4.5. Audit Log Backup Procedures

Logs are periodically backed up on-site and off-site pursuant to backup procedures.

5.4.6. Audit Collection System (Internal vs. External)

Audit logs are kept by the CA management software used in carrying out CA business processes.

5.4.7. Notification to Event-Causing Subject

Where audit logs are created other than routine operations, the event causing subject is warned by the system. Depending on the type and significance of the event, the system may also inform person(s) who may have higher authority level in charge of the subject causing the event.

5.4.8. Vulnerability Assessments

Audit logs are reported on the system. By analyzing these reports, security gaps in the system and fault points in certification processes shall be identified and measures shall be taken.

5.5. Records Archival

5.5.1. Types of Records Archived

Pursuant to TÜRKTRUST's operation, all audit logs stated in Article 5.4, applications, requests and instructions relating to certification processes, all supporting documents obtained on paper and subscriber's agreement, all correspondence with customers, all generated certificates and CRLs, all versions of CP and CPS documents, all practice procedures, instructions and forms shall be archived according to the TÜRKTRUST archival procedures. While a large portion of archives is retained in electronic medium, such materials kept on paper as correspondence; forms, documents, customer files and company information are archived in paper medium.

5.5.2. Retention Period for Archive

Archives relating to TÜRKTRUST's operation regarding qualified electronic certificates shall be retained for at least 20 (twenty) years. Archives regarding server and object signing certificates shall also be retained for 20 (twenty) years by TÜRKTRUST. Logs of operations for trial certificates are not retained.

5.5.3. Protection of Archive

Archives are protected by physical and electronic security measures, and kept open for access by authorized personnel only.

Electronic archives are protected against unauthorized viewing, modification or deletion. Archives on paper are retained in special units to which only authorized personnel can access.

5.5.4. Archive Backup Procedures

Backups of electronic archives are retained pursuant to backup procedures. No backup is made for archives on paper.

5.5.5. Requirements for Time-Stamping of Records

All electronic archive records kept by TÜRKTRUST are time-stamped.

5.5.6. Archive Collection System

Archive logs are collected using the TÜRKTRUST archive management system.

5.5.7. Procedures to Obtain and Verify Archive Information

Controlled access is provided for TÜRKTRUST's archives upon the request of the Institution or as required by laws.

5.6. Key Changeover

Re-keying actions for root and subroot certificates of the issuing certification authorities under TÜRKTRUST shall be administered by the TÜRKTRUST center.

Where the expiry of a root certificate draws closer, the term of an end user certificate to be issued shall be designated not to go beyond the expiry of any of the associated root certificates. For the period when the term of the old root certificate and that of the renewed root certificate overlaps, TÜRKTRUST makes a cross-certification for these two root certificates so that certificates issued based on both roots may be used smoothly; and such cross-certification shall be appropriately notified to subjects and relying people.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Where events or security compromises occur which would prevent TÜRKTRUST's operations, intervention is made pursuant to TÜRKTRUST's disaster management procedures and business continuity plans.

5.7.2. Computing Resources, Software and/or Data Are Corrupted

Where computing resources are damaged, software units or operational data are corrupted, the damaged hardware in the facility shall first be made up and running again. Then, lost records shall be re-created by backup systems and certification services shall be re-activated. If it cannot be made fully operational or some of the records cannot be re-created, all subscribers and relying people that may be affected shall be urgently notified. Where necessary, certain certificates shall be revoked and new certificates shall be issued.

5.7.3. Entity Private Key Compromise Procedures

Where security and trustworthiness of TÜRKTRUST private keys are compromised, the relevant certificates shall be revoked pursuant to TÜRKTRUST's disaster management procedures and business continuity plans and new private keys shall be generated and enabled pursuant to Article 5.6. New certificates shall be issued to replace the revoked certificates according to procedures and all subscribers and relying people that may be affected shall be urgently notified.

5.7.4. Business Continuity Capabilities after a Disaster

Where events or security compromises occur which would prevent TÜRKTRUST's operations, intervention is made pursuant to TÜRKTRUST's disaster management procedures and business continuity plans.

5.8. TÜRKTRUST or Registration Authority Termination

Electronic and paper records relating to all certificate application and registration operations made by registration authorities are retained at the TÜRKTRUST center to complete certificate applications and action requests. Therefore, where the operation of a registration authority is terminated, records retained in that registration authority shall be destroyed.

Where TÜRKTRUST is to terminate its certification services, it shall notify this case to the Institution and announce to the public at least 3 months in advance pursuant to the Law and the Regulation. TÜRKTRUST shall, pursuant to the termination of operations procedures, turn over to another CA all data, documents and records relating to the existing certificates within one month pursuant to the Law. The Institution may allow an extension of no more than one month if so deems appropriate. If the turn over operations could not be completed within the specified time, TÜRKTRUST shall revoke relevant certificates and notify all relevant parties. In such case, TÜRKTRUST generates the last CRL log and destroys its own private key and backups.

6. TECHNICAL SECURITY CONTROLS

This section of the CPS document describes security controls for the management of private keys and activation data used in business processes relating to TÜRKTRUST certification services and for the technical infrastructure and certification services operation.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Private keys and public keys of subjects of qualified electronic certificates may be generated on the TÜRKTRUST side or the customer side. Where generation takes place on the TÜRKTRUST side, the operation is performed in the issuing certification authority in hardware security modules that have appropriate security levels. In such case, private keys of customers shall not be stored at TÜRKTRUST, no copies are taken. Alternatively, an applicant who acquires a secure electronic signature creation device may generate the private and public keys pursuant to the related TÜRKTRUST certification application methods.

Private and public key pairs for server and object signing certificates are generated in the server under the control of the applicant.

Key pairs for trial certificates are generated by the client software of the applicant or the signature creation device owned by the applicant during automatic certificate generation. It is not required that private keys of trial certificates should be generated or stored in secure electronic signature creation devices.

Key pairs for TÜRKTRUST root and subroot certificates shall be generated pursuant to the TÜRKTRUST procedures for key generation for root certificates under the control of authorized personnel only in environments technically and administratively secured. Private keys are protected against unauthorized access by physical and technical security measures.

In all cases where TÜRKTRUST handles key generation, key pairs are generated in hardware security modules that have appropriate security levels.

Applicants of qualified electronic certificates who generate the key pairs on their side are responsible for using the secure electronic signature creation devices.

Server administrators who apply for server certificates and technical responsibles that apply for object signing certificates are responsible for conducting the key generation securely during the applications for server certificates.

6.1.2. Private Key Delivery to Subscriber

For qualified electronic certificates for which key pairs are generated by TÜRKTRUST, the private keys shall be dispatched inside the secure electronic signature creation devices to be delivered by courier to subscribers against identification checks and hand written signatures. Activation data for the secure electronic signature creation devices shall be separately delivered by courier to subscribers against identification checks and hand written signatures.

Since private keys of server certificates and trial certificates are generated on the customer side, they are under the responsibility of the applicants.

6.1.3. Public Key Delivery to Certificate Issuer

Where key pair generation takes place on the customer side, the certificate request has to be signed by the private key corresponding to the public key. Thus, it would be possible to detect an alteration in the content of the request. To prevent third parties accessing the request information, the request shall be communicated to TÜRKTRUST through electronic communications.

6.1.4. TÜRKTRUST Public Key Delivery to Relying People

TÜRKTRUST root and subroot certificates are published at http://www.TÜRKTRUST.com.tr accessible by relying people. The SHA-1 hash for these certificates shall be published in three (3) most circulated newspapers in Turkey. Thus, relying people may use public keys of TÜRKTRUST.

6.1.5. Key Sizes

TÜRKTRUST certificates comply with minimum key lengths specified in the Communiqué.

TÜRKTRUST's root and subroot certificates are at least 2048 bit length when and if RSA keys are used.

For all end user certificates issued by TÜRKTRUST, at least 1024 bit RSA key pairs are used.

6.1.6. Key Generation and Quality Checking

Where key generation takes place at the TÜRKTRUST center, key pairs are generated in hardware security modules that have appropriate security levels in accordance with the parameters specified in the Communiqué.

Where key generation takes place on the customer side, the customer is responsible for generating the private key in appropriate tools and quality.

6.1.7. Key Usage Purposes

End user keys generated under TÜRKTRUST certification services shall be used for authentication and electronic signature purposes.

Keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities shall be used for signing certificates and CRLs.

Usage purposes of keys are indicated in key usage fields of X.509 v3 certificates.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Key pair generation and certificate and CRL signing operations at TÜRKTRUST are realized in secure cryptographic hardware modules conforming to the standards specified in the Communiqué.

Where private keys of subscribers of qualified electronic certificates are generated on the TÜRKTRUST side, they are loaded into smart cards, smart bars and similar secure electronic signature creation devices conforming to the standards specified in the Communiqué. Private keys in the secure electronic signature creation devices are prevented from removal, modification or reproduction. Where a certificate applicant generates the key on his side, he should use a tool that has security levels defined in the Communiqué.

6.2.2. Private Key Multi-Person Control

Unauthorized access is prohibited to root and subroot certificates of issuing certification authorities under TÜRKTRUST. In addition to physical and technical access controls, the use of such private keys is only possible by two separate authorized persons connecting to the relevant module and approval by the system. It is never allowed in the system that one single authorized person alone can use TÜRKTRUST's private keys.

Private keys of qualified electronic certificates shall be stored only in the password controlled, secure electronic signature creation devices which are under the responsibility of subscribers. Private keys cannot be used unless the password to the tool is known. Password security is ensured by the tool's hardware.

Server administrators and technical responsibles are responsible for ensuring security for private keys of server certificates and object signing certificates, respectively.

Hardware control shall not apply to trial certificates.

6.2.3. Private Key Escrow

Private keys of end user certificates issued by TÜRKTRUST are strictly not escrowed by TÜRKTRUST, nor are such keys copied.

6.2.4. Private Key Backup

Private keys of end user certificates issued by TÜRKTRUST are not backed up, or copied. Private keys of qualified electronic certificates, server certificates, object signing certificates and trial certificates are under the responsibility of subscribers, server administrators and technical responsibles.

In order to ensure continuity of services in case of a disaster or a problem, the private keys of root and subroot certificates of TÜRKTRUST's issuing certification centers are kept under physical and technical security controls with respect to TÜRKTRUST root certificates key production procedure.

6.2.5. Private Key Archival

Not applicable.

6.2.6. Private Key Transfer into or from a Cryptographic Module

Private keys of CA root and subroot certificates are generated in secure cryptographic hardware modules. These keys cannot in any way be taken out of the module except for transfer into secure modules used for backup purposes. The backup operation is realized in encrypted form on the cryptographic hardware module.

Where key generation takes place on the TÜRKTRUST side, the key pair is generated in the secure cryptographic hardware modules that have appropriate security levels and transported to the secure electronic signature creation devices of subscribers of qualified electronic certificates.

Where key generation takes place on the customer side, it is the customer's responsibility to ensure control of private key and its security during a possible transfer.

6.2.7. Private Key Storage on Cryptographic Module

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities are stored on cryptographic hardware modules where they are generated and which have security levels specified in the Communiqué.

Where private keys of subscribers of qualified electronic certificates are generated on the TÜRKTRUST side, they are stored on cryptographic hardware modules where they are generated and which have security levels specified in the Communiqué. Private keys in the secure electronic signature creation devices are prevented from removal, modification or reproduction.

Where a certificate applicant generates the key on his side, he should use a tool that has security levels defined in the Communiqué.

Server administrators and technical responsibles are responsible for securely storing private keys of server certificates and object signing certificates in the servers where they are generated.

Subscribers are responsible for storing private keys of trial certificates.

6.2.8. Method of Activating Private Key

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities shall be activated in the presence of two authorized on the hardware security module in which they are.

Private keys of qualified electronic certificates shall be activated by entering password to the secure electronic signature creation device.

Private keys of server and object signing certificates shall be activated on the client software.

The method of activation for private keys of trial certificates are under the control of customers.

6.2.9. Method of Deactivating Private Key

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities shall be activated only for a certain length of time and a specific operation on the hardware security module in which they are, and deactivated upon completion of the operation or expiry of the time. To use the private keys again, the authorized persons should be identified to the system and the private keys should be activated again.

Private keys of qualified electronic certificates shall be activated for a certain length of time upon password entry to the secure electronic signature creation device, and deactivated at the expiry of the time. Also, the subscriber may, at his will, deactivate the private key. To use the private key again, the subscriber should enter the password to the secure electronic signature creation device.

Private keys of server certificates, object signing certificates and trial certificates shall be made through the client software.

6.2.10. Method of Destroying Private Key

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities may be destroyed only by authorized persons using the zeroization function of hardware security modules in which they are. For this operation, at least two persons should be present.

Private keys associated with qualified electronic certificates and stored in the secure electronic signature creation devices could be destroyed by hardware using the management software of the device.

There is no stipulation for destroying private keys of end user certificates upon certificate revocation or expiry. The subscriber, the server administrator or the technical responsible may destroy the private key if he so wishes.

6.2.11. Cryptographic Module Rating

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities are generated in cryptographic hardware modules that have security levels specified in the Communiqué.

Private keys of qualified electronic certificates are stored in secure electronic signature creation devices that have security levels specified in the Communiqué.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public keys associated with root and subroot certificates of TÜRKTRUST's issuing certification authorities are stored for 20 years by the CA.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The term for qualified electronic certificates, server certificates and object signing certificates issued by TÜRKTRUST is 1 (one), 2 (two) or 3 (three) year(s), and for trial certificates 3 (three) months. Term for key pairs used for 1 (one) year qualified electronic certificates cannot exceed 3 years.

The term for root and subroot certificates of TÜRKTRUST's issuing certification authorities cannot exceed 10 (ten) years. At the end of this term, re-keying shall absolutely take place when certificates are renewed.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities or cryptographic modules in which such keys are located may be accessed by the activation data in the presence of two authorized persons.

Activation data for private keys of TÜRKTRUST's authorized persons and subscribers of qualified electronic certificates are generated during certificate issuance and printed into sealed envelope and transmitted. These persons may, at any time, change these passwords which are solely under their control.

Server administrators and technical responsibles hold the activation data for private keys of server and object signing certificates. Activation data for private keys of trial certificates shall be generated on the customer side.

6.4.2. Activation Data Protection

Since activation data for private keys of TÜRKTRUST's subscribers of qualified electronic certificates are generated during certificate issuance and printed into sealed envelope and transmitted to them, such data are under their control. There is no copy of such activation data, nor stored by TÜRKTRUST. Subscribers may change activations data any time they wish and it is recommended they should do so. After delivery of activation data to subscribers, they are responsible for ensuring their confidentiality and security.

TÜRKTRUST's authorized persons are responsible for changing the activation data for their private keys at indicated frequency pursuant to the security procedures and ensuring that such data should not be known to others.

Server administrators, technical responsibles and subscribers should ensure confidentiality and security of the activation data for private keys of server certificates, object signing certificates and trial certificates respectively.

6.4.3. Other Aspects of Activation Data

Pursuant to the process of qualified electronic certificate issuance and distribution where activation data are generated and transmitted to subscribers by TÜRKTRUST, such data are printed in sealed envelopes and transmitted by courier to subscribers as separate from the secure electronic signature creation device. The separate transmission of the signature creation device and activation data is a security measure against loss, disclosure or acquisition by unintended persons. To ensure secure transmission by courier, TÜRKTRUST signs a service contract with the courier company in which security clauses and responsibilities are explicitly stipulated.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Under the certification business processes carried out by TÜRKTRUST, the following security controls are implemented to access and operate all information systems:

- Computer systems utilize secure and certified hardware and software products.
- Computer systems are protected against unauthorized access and security gaps. Controls for penetration and intrusion have been established and such controls have been validated by relevant tests and ensured for continuity.
- Computer systems are protected against network security hacking.
- Access rights to computer systems and authentication are ensured by passwords supplied to TÜRKTRUST's personnel.
- Access rights to computers have been limited to the roles assigned to authorized persons.
- Data communications are handled securely between the units that make up the computer system.
- Since operational records are constantly logged, problems that may arise in the computer systems can be identified in short time and accurately.

6.5.2. Computer Security Rating

Not applicable.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Not applicable.

6.6.2. Security Management Controls

Appropriate tools are used and security procedures are implemented to ensure security of the operational systems and the computer network used in TÜRKTRUST.

TÜRKTRUST holds the ISO/IEC 27001 Information Security Management Systems Standard certificate.

6.6.3. Life Cycle Security Controls

Not applicable.

6.7. Network Security Controls

Private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities are used in environments where network security is ensured. Such systems are protected physically and technically.

All other systems within TÜRKTRUST are also protected by appropriate network security methods. All network elements such as firewalls, keying devices and routers have been installed correctly and securely in accordance with the network configuration procedures. Security controls of such network elements are constantly made pursuant to the procedures.

Registration authorities under TÜRKTRUST communicate records relating to their certification operations to TÜRKTRUST over the Internet by secure network connection.

6.8. Time-Stamping

During the execution of certification services of TÜRKTRUST, electronical records for certain operations contain time information synchronized by time source used for time-stamping services. Data integrity is preserved by keyed hash method and time-stamping is used at the archiving phase.

7. CERTIFICATE, CERTIFICATE REVOCATION LIST (CRL) AND OCSP PROFILES

This section of the CPS document describes the profiles of certificates issued and CRLs generated, and the structure of OCSP service by TÜRKTRUST.

7.1. Certificate Profile

TÜRKTRUST certificates basically contain the following fields:

- Subscriber information (name, company, department, place, country, e-mail etc.)
- Server information on server certificates (domain name, server name, company name etc.)
- Subscriber information on object signing certificates (firm, working unit etc.)
- TÜRKTRUST Certification Authority information with the country name TR (Turkey)
- Start and end dates of certificate's validity period
- Electronic signature creation algorithms used
- Public key of subscriber
- Certificate's serial number
- Signature of TÜRKTRUST Certification Authority

Qualified electronic certificates issued by TÜRKTRUST also contain the following information as required by the Law:

- An indication that the certificate is a "qualified electronic certificate"
- If the subscriber is acting on behalf of another person, information on such authority
- Professional and other personal information if the subscriber so requests
- If any, usage conditions of the certificate and limits of material transactions on certificate usage.

7.1.1. Version Numbers

Root and subroot certificates and end user certificates issued by TÜRKTRUST support the X.509 v3 version pursuant to the "IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002" document.

7.1.2. Certificate Extensions

TÜRKTRUST supports all certificate extensions defined under RFC 3280 - X.509 v3 standard. According to the certificate type, key usage, certificate policies extension, subject alternative names, basic constraints, extended key usage, CRL distribution points, authority key identifier, subject key identifier extensions are appropriately set up.

Qualified electronic certificates contain the qualified electronic certificate extensions defined under the "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile, January 2001" document.

7.1.3. Algorithm Object Identifiers

SHA-1 is used as the hashing algorithm in certificates issued by TÜRKTRUST, and RSA is used for generating public and private keys and electronic signature. Object identifiers of algorithms used are indicated in the respective field of the issued certificates.

7.1.4. Name Forms

Certificates issued by TÜRKTRUST use X.500 distinguished names.

7.1.5. Name Constraints

No anonymity or pseudonyms shall be used in qualified electronic certificates issued by TÜRKTRUST. T.R. identity numbers are used as a distinguishing feature in the names.

7.1.6. Certificate Policy Object Identifier

In the "certificate policy" extension of certificates issued by TÜRKTRUST, the relevant certificate policy object identifier number (OID) indicated in Article 1.2 of this CPS document is used by the certificate type.

7.1.7. Usage of Policy Constraints Extension

TÜRKTRUST's subroot certificates may contain policy constraints extension as necessary.

7.1.8. Policy Qualifiers Syntax

In the "certificate policy" extension of certificates issued by TÜRKTRUST, the access information for the CPS document has been provided as policy qualifier in URL form.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2. CRL Profile

CRLs generated by TÜRKTRUST basically contain TÜRKTRUST's electronic signature and publisher's information, CRL's date of publication, date of publication for the next CRL, and serial numbers of revoked certificates and dates and times of revocation.

7.2.1. Version Number

CRLs generated by TÜRKTRUST support the X.509 v2 version under the "IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002" document.

7.2.2. CRL and CRL Entry Extensions

CRLs generated by TÜRKTRUST use extensions defined in RFC 3280.

7.3. OCSP Profile

TÜRKTRUST provides uninterrupted on-line certificate status protocol OCSP support which is a real time certificate status inquiry. By this service, when appropriate certificate status inquiries are received, the status of certificates and additional information as required by the protocol are returned to the inquirer as the response.

7.3.1. Version Number

The OCSP service provided by TÜRKTRUST supports the v1 protocol version under the "IETF RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1999" document.

7.3.2. OCSP Extension

In the content of OCSP service provided by TÜRKTRUST, extensions defined in RFC 2560 may be used. However, it is not mandatory to use all extensions other than the basic OCSP information.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TÜRKTRUST is audited by the Telecommunication Authority under the respective legislation.

In addition, all CA processes are subject to periodical compliance audit, in terms of continuity of the information security management system, pursuant to the ISO/IEC 27001 Information Security Management System certificate.

Provision of CA services and security circumstances of operation are controlled under an internal audit plan.

8.1. Frequency and Circumstances of Assessment

The Telecommunication Authority, as the regulating and auditing Agency, conducts audits as it deems necessary ex officio. During the audit, it is mandatory that certification authorities and relevant persons fulfill the requests of auditors in providing all books, documents, and records, access to management premises, buildings and extensions, taking written and verbal information, taking samples, and auditing operations and accounts.

All CA processes are subject every year to periodical compliance audit, in terms of continuity of the information security management system, pursuant to the ISO/IEC 27001 Information Security Management System certificate. This certification is renewed every three years.

Internal audit is conducted at least once a year according to the plan, and more frequently if deemed necessary.

8.2. Identification and Qualifications of Assessor

The Telecommunication Authority is the regulating and auditing agency designated by the Law.

The ISO/IEC 27001 Information Security Management System certification shall be conducted by an authorized assessor.

TÜRKTRUST's institutional audit is conducted by TÜRKTRUST's authorized personnel. The internal audit is conducted by the Information Security Management System and Quality Management System personnel within TÜRKTRUST.

8.3. Assessor's Relationship to Assessed Entity

The Institution which is the auditor is the regulatory organization authorized by the Law to audit all CAs operating in the field of qualified electronic certificates in Turkey.,

The ISO/IEC 27001 Information Security Management System certification shall be conducted by an independent, authorized assessor.

TÜRKTRUST's institutional audit is conducted by TÜRKTRUST's authorized personnel.

8.4. Topics Covered by Assessment

The audit by the Institution covers, within the framework of authority entrusted by the Law, all processes relating to TÜRKTRUST's electronic certification services, technical infrastructures used in providing such services and the facilities where such services are provided.

The ISO/IEC 27001 Information Security Management System certification covers TÜRKTRUST's electronic certification and time-stamping services.

The internal audit covers all matters that fall under the legal audit.

8.5. Actions Taken as a Result of Deficiency

During the audits conducted by the Institution pursuant to the Regulation, if any matter so significant as to adversely affect TÜRKTRUST's activities and operation are found out, sanctions and penalties are imposed as indicated in the legislation.

Any deficiencies found out during the ISO/IEC 27001 Information Security Management System may lead to revocation of the certificate if such deficiencies are of major extent. Minor deficiencies shall be remedied by TÜRKTRUST until the next audit.

Deficiencies detected in the internal audits conducted by TÜRKTRUST are remedied and preventive measures are taken.

8.6. Communication of Results

The results of the audit conducted by the Institution pursuant to the Law shall be communicated officially to TÜRKTRUST if deemed necessary. Non-communication of any result from the Institution means there is no adverse assessment.

The ISO/IEC 27001 Information Security Management System audit results shall be communicated officially to TÜRKTRUST by the assessor.

The results of the internal audit are included in the internal audit reports and submitted to evaluation by the relevant authorized persons.

9. OTHER BUSINESS AND LEGAL MATTERS

This section of the CPS document describes TÜRKTRUST's commercial and legal practice and service conditions that should be fulfilled for certification processes.

9.1. Fees

9.1.1. Certificate Issuance and Renewal Fees

Certificates issued by TÜRKTRUST are priced differently depending on type.

Qualified electronic certificates are priced to the extent of material transaction limits included, and according to certificate generation costs and market conditions. A higher material transaction limit is reflected to the certificate prices at the higher certificate financial liability insurance premiums.

Server certificates and object signing certificates are priced according to certificate type, term and characteristics.

Trial certificates are free of charge.

Updated certificate price schedules are announced to customers at the TÜRKTRUST website and through other appropriate communication channels.

9.1.2. Certificate Access Fees

Certificates issued by TÜRKTRUST are kept accessible to the public provided that subjects consent in writing.

No fees shall be charged for certificate access services.

9.1.3. Revocation or Status Information Access Fees

Revocation or status information for certificates issued by TÜRKTRUST are kept accessible to relying people by way of CRLs and OCSP service.

No fees shall be charged for access services to revocation or status information for qualified electronic certificates as required by the Law.

Access services on revocation or status information provided by TÜRKTRUST for server certificates, object signing certificates and trial certificates are also free of charge.

9.1.4. Fees for Other Services

TÜRKTRUST does not charge fees for manuals and documents such as CP, CPS, subscriber's and certificate services commitments published to the public.

Fees for other products and services which are offered to customers with added value are announced to customers at the website and through other appropriate communication channels.

9.1.5. Refund Policy

TÜRKTRUST does not refund for qualified electronic certificates, server certificates and object signing certificates. However, if the certificate contains information different than that on the application due to causes attributable to TÜRKTRUST, a new certificate shall be issued free of charge.

9.2. Financial Responsibility

TÜRKTRUST is under obligation to carry certificate financial liability insurance to cover the damages that would arise from its failure to perform its obligations under the Law. Conditions regarding the insurance are included in the "Certificate Financial Insurance Liability Regulation" promulgated in the Official Gazette dated 26 August 2004 issue 25565 and respective communiqués.

9.2.1. Insurance Coverage

Pursuant to Article 6 of the "Certificate Financial Insurance Liability Regulation," certificate financial liability insurance insures the CA for legal liabilities against those suffering damages that may arise from its failure to fulfill its obligations to use secure products and systems, provide services securely, prevent imitation and falsification.

Qualified electronic certificates issued by TÜRKTRUST are covered by insurance.

No material transactions may be made by trial certificates; no insurance coverage is provided to such certificates.

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End-Users

TÜRKTRUST is under obligation to buy the certificate financial liability insurance for the qualified electronic certificate to cover damages arising from its failure to fulfill its legal obligations prior to delivering the certificate to the subscriber.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following are included in the scope of confidential information: all confidential commercial information and documents relating to TÜRKTRUST's certification services, private keys of root and subroot certificates of TÜRKTRUST's issuing certification authorities, software and hardware information, operational records, audit reports, access passwords to on-site areas and devices, facility layout and interior design, emergency action plans, business plans, sales data, cooperation agreements, confidential information of business partner organizations.

9.3.2. Information Not Within the Scope of Confidential Information

Information and documents of TÜRKTRUST which are not commercially confidential, and which should be kept public pursuant to the Law and practices shall be excluded from the scope of confidential information. Certificates issued, CRLs, customer guides relating to certification services, the CP document, the CPS document, information included in subscriber's and certificates services commitments are not confidential.

9.3.3. Responsibility to Protect Confidential Information

All TÜRKTRUST employees have responsibility in protecting confidential information. Pursuant to security policies, no person or third party other than the authorized employee is allowed to access any confidential information. All procedures relating to ensuring information security are strictly applied and such application is subject to TÜRKTRUST's internal audit.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

TÜRKTRUST, in the scope of certification services provided, protects privacy of personal information of certificate applicants, subscribers or other participants.

9.4.2. Information Treated as Private

Information and documents for identity validation received from certificate applicants and needed during the certification services provided by TÜRKTRUST shall be used for certification services, and such customer information as demographic information, communications information not included in the certificate's content is deemed private information.

9.4.3. Information Not Deemed Private

Information included in the certificates of subscribers who are TÜRKTRUST's customers and announced to relying people along with the certificates is not deemed private unless otherwise requested by the subscriber.

9.4.4. Responsibility to Protect Private Information

All TÜRKTRUST employees have responsibility in protecting private information of applicants and customers. No person or third party other than the authorized employee is allowed to access any private information.

9.4.5. Notice and Consent to Use Private Information

Not applicable.

9.4.6. Disclosure Pursuant to Judicial and Administrative Process

Private information required in the judicial and administrative processes shall be given only to the requesting authority.

9.4.7. Other Information Disclosure Circumstances

Not applicable.

9.5. Intellectual Property Rights

TÜRKTRUST holds the intellectual property rights on all certificates issued by TÜRKTRUST, CRLs, customer guides relating to certification services, CP and CPS documents, subscriber's and certificate services commitments, all internal and external documents relating to certification services, databases, websites and all products developed in association with certification services.

Certificate subscribers hold the property rights on all distinguishing names and marks included in the certificate's content and owned by the subscriber.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Issuing certification authorities under TÜRKTRUST represent and warrant that contents of all issued certificates are accurate, identity validation steps have been performed accurately and reliably, the right certificate has been issued to the right applicant and delivered to the right person, published certificate status information is updated and accurate, and they will perform all practice requirements and obligations included in CP and CPS.

Issuing certification authorities under TÜRKTRUST fulfill CA obligations stated in Article 10 of the Law and Article 14 of the Regulation to issue qualified electronic certificates.

9.6.2. Registration authority Representations and Warranties

Registration centers under TÜRKTRUST represent and warrant that identity validation have been performed accurately and reliably for the applicants, records are kept accurately, certificate issuing, renewal and revocation requests transmitted to the CA center have been accurate and complete.

9.6.3. Subscriber Representations and Warranties

Subscribers represent and warrant that they will furnish updated and accurate information and documents to TÜRKTRUST during certificate application and renewal and revocation requests, use their certificates under the conditions stated in the CP and CPS documents, and fulfill all obligations stipulated in the subscriber’s agreement.

Subscribers of qualified electronic certificates have to fulfill obligations stated in Article 15 of the Regulation along with the stipulations in the subscriber’s agreement.

9.6.4. Relying People Representations and Warranties

Subscribers and relying people are under obligation to check the validity of electronic signature generated based on TÜRKTRUST’s qualified electronic certificates.

9.6.5. Representations and Warranties of Other Participants

Other participants which are comprised of all persons and organizations which TÜRKTRUST cooperates with and from which TÜRKTRUST procures services during certification services represent and warrant that they provide the services reliably and accurately and not disclose confidential or private information regarding TÜRKTRUST’s processes and customers. TÜRKTRUST signs service contracts with service providing organizations in which such representations and warranties are explicitly stipulated.

9.7. Disclaimers of Warranties

Not applicable.

9.8. Limitations of Liability

Certificates issued by TÜRKTRUST are insured within the material transaction limits for money transactions. Limits of liability regarding the certificates and usages are explicitly stipulated in the subscriber’s commitment.

9.9. Indemnities

If TÜRKTRUST fails to fulfill its obligations pursuant to the policies and principles in the CP and this CPS and third parties suffer damages due to such failure, TÜRKTRUST shall indemnify any such damage.

Pursuant to Article 13 of the Law, TÜRKTRUST is under obligation to indemnify the damages it inflicts to third parties under qualified electronic certificate services by way of violation of the Law and Regulation. In such cases, if TÜRKTRUST proves its faultlessness, then it is relieved of such obligation of indemnification.

Where subscribers fail to fulfill their obligations under the subscriber’s agreement and TÜRKTRUST and/or third parties suffer damages due to such failure, the subscriber shall indemnify such damage. The indemnification clause is included in the subscriber’s commitment.

9.10. Term and Termination of CPS Documentation

9.10.1. Term

This version of the CPS document is valid until a new version is available.

9.10.2. Termination

Where a situation arises that require changing the content of the present version of this CPS document depending on changes and arrangements that may occur in TÜRKTRUST's activities and certification services, this document may become partially or wholly invalid. In such case, a new CPS document version which covers relevant changes shall be prepared and published by TÜRKTRUST.

9.10.3. Effect of Termination and Survival

Where the validity of the present CPS version terminates, necessary measures are taken to ensure continuity of TÜRKTRUST's activities and certification services. The new CPS version is prepared before the validity of the old CPS version terminates and the change shall be realized without interruption of service.

Where it becomes necessary to make changes in certificates issued by TÜRKTRUST due to the aforesaid changes, subscribers and relying people shall be notified and necessary actions are completed rapidly. Practices that have changed due to the new version shall be immediately implemented by TÜRKTRUST.

9.11. Individual Notices and Communications to Participants

All individual notices from TÜRKTRUST to subscribers shall be made by e-mail. Official papers can be sent as a notice for necessary situations.

Notices from TÜRKTRUST to relying people shall be published over the web or press media.

9.12. Amendments

Where a situation arises that require changing the content of the present version of this CPS document depending on changes and arrangements that may occur in TÜRKTRUST's activities and certification services, a new CPS document version which covers relevant changes shall be prepared and published by TÜRKTRUST.

While the CPS document undergo minor changes that would not affect the use and acceptability of certificates issued earlier, there may be significant changes that would directly affect certificate use. TÜRKTRUST practice differs for two cases.

9.12.1. Amendment Procedure

Where a situation arises that require amending the content of the present version of this CPS document depending on changes and arrangements that may occur in TÜRKTRUST's activities and certification services, a new CPS document version which covers relevant changes shall be prepared and published by TÜRKTRUST.

Amendments to CP shall be reflected onto the relevant practices in CPS. Therefore, a new CP version necessitates a new CPS version. The access data to the CPS document given as URL in the "certificate policy" extension of certificates issued by TÜRKTRUST shall remain the same, but the CPS document indicated by this address is the new version.

Where minor amendments occur, certificates issued earlier shall continue to be used in accordance with the new CP and CPS documents. However, if a new CP version is issued due to significant amendments, the certificates issued earlier which are associated with the amended certificate policy may not be used compatibly with the new CP.

9.12.2. Notification Mechanism and Period

Where changes in TÜRKTRUST's activities and certification services and amendments to the present CP and CPS documents occur, subscribers and relying people shall be immediately notified on the updated CP and CPS versions issued.

Particularly in significant amendments, since the usability and acceptability of the certificate may be affected in some applications, TÜRKTRUST shall use all reasonable means to notify subscribers and relying people. The amendment shall be published in the TÜRKTRUST website, subscribers are contacted directly through communication information, and where necessary all relying people are informed through the press media.

Minor changes are announced in the web site and subscribers are notified by e-mail.

The new CP and CPS versions shall be published in the TÜRKTRUST repository along with the old versions to include detailed version information and kept accessible to relevant parties.

9.12.3. Circumstances under Which OID Must Be Changed

Significant changes realizing in a way that crucially affecting the authentication steps used or the security level of certificate in certificate services, which could directly affect certificate usage and acceptability require that object identifier numbers of the relevant certificate policy defined in the CP document may be changed. In this case, new certificates contain object identifier numbers of the new certificate policy to be implemented.

9.13. Dispute Resolution

Where disputes arise between TÜRKTRUST and subscribers and relying people, efforts shall be made to settle such disputes pursuant to the policy and principles laid down in the CP and CPS documents, procedures, commitments and contracts.

Actions relating to qualified electronic certificates shall be conducted under the Law and the Regulation and associated Communiqués.

If disputes could not be amicably settled, then Ankara Courts have jurisdiction for resolution of disputes.

9.14. Governing Law

The use of electronic signature in Turkey which gives the same consequence as of manual signature is regulated by the "Electronic Signature Law" no.5070 and the Regulation and Communiqués issued by the Telecommunication Authority. The Institution is responsible for regulating and auditing the CA's operations under the Law.

9.15. Compliance with Applicable Law

TÜRKTRUST provides qualified electronic certificate services in accordance with the "Electronic Signature Law" no.5070 and the Regulation and Communiqués issued by the Telecommunication Authority.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Not applicable.

9.16.2. Assignment

Not applicable.

9.16.3. Severability

Where any section of the CP and CPS documents become invalid in a manner not to affect the validity of other sections, the unaffected other sections shall remain valid and in effect and be implemented until the new versions are issued by TÜRKTRUST which reflect the changes.

9.16.4. Waiver of Rights

Not applicable.

9.16.5. Force Majeure

Any circumstance which obstructs TÜRKTRUST’s performance of activities relating to electronic certification service provision and is normally beyond TÜRKTRUST’s control is called a force majeur. While such forces majeurs continue to be effective, TÜRKTRUST’s activities may be interrupted or experience problems. Natural disasters, wars, acts of terrorism, failures in telecommunication, Internet and similar infrastructures are deemed forces majeurs.

9.17. Other Provisions

Not applicable.