CERTIFICATE POLICY (CP)

VERSION : 07

DATE : 15.07.2013

1. INTRODUCTION

TURKTRUST Information, Communications and Information Security Services Inc. (hereinafter "TURKTRUST") 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 secondary legislation issued by the Information and Communication Technologies Authority.

This documentation named the Certificate Policy (CP) has been prepared by TURKTRUST, in order to identify the policies and rules to be followed in the course of activities of TURKTRUST certificate services, 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 Information and Communication Technology Authority under the Law.

Regarding SSL (Secure Socket Layer) Certificate and EV (Extended Validation) SSL Certificate services, TURKTRUST conforms to the current version of the "ETSI TS 102 042 Electronic Signatures Infrastructure (ESI); Policy Requirements for Certification Authorities Issuing Public Key Certificates". Moreover, for SSL and EV SSL certificates TURKTRUST conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document published at http://www.cabforum.org and referenced from the ETSI TS 102 042 standard. For EV SSL certificates requiring extended validation, TURKTRUST also conforms to the current version of the "CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates" document again published at http://www.cabforum.org and referenced from the ETSI TS 102 042 standard. In the event of any inconsistency between this CPS document and those ETSI TS 102 042, Baseline Requirements and EV Guidelines documents, the requirements in those documents take precedence over this CPS document. Compliance to those documents includes "Publicly-Trusted Certificate Policy - Baseline Requirements (PTC-BR)" and "Extended Validation Certificate Policy (EVCP)" found in the ETSI TS 102 042 standard.

This CP document lays down all administrative, technical and legal requirements related with certificate applications, certificate issuance and management, certificate renewal and certificate revocation procedures and specifies the implementation responsibilities of TURKTRUST as the certification authority ("CA") (or, electronic certificate service provider), subscribers and relying parties.

1.1. Overview

This CP document covers all electronic certificate services provided by TURKTRUST. The policies and rules included in CP cover all of TURKTRUST's customer services, registration authorities and issuing certification authorities.

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

TURKTRUST evaluates its Certificate Policy and Certification Practice Statement documents in accordance with related legislation and standards at least once a year in the management review meeting. As a consequence of this evaluation or due to any requirements arising throughout the year, those documents are revised if necessary.

1.2. Document Name and Identification

This CP document is named as the "TURKTRUST Certificate Policy (CP)". The version number and date of the document is provided herein on the cover page.

TURKTRUST, acting as the policy-defining authority for certification services in accordance with this CP document, has taken the unique corporate object identifier "2.16.792.3.0.3" from Turkish Standards Institution. TURKTRUST has assigned an object identifier value extension under TURKTRUST corporate object identifier for the following certificate types set forth in the CP.

- TURKTRUST QEC 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 signatures of individuals pursuant to the Law, the Regulation and the Communiqué. Qualified electronic certificates aimed for mobile signature usage are also bound by the same policies.
- TURKTRUST SSL Certificate Policy (2.16.792.3.0.3.1.1.2) covers SSL certificates for servers. SSL Certificates are issued and maintained in conformity with "Normalized Certificate Policy" defined in ETSI TS 102 042.
- TURKTRUST OSC Policy (2.16.792.3.0.3.1.1.4) covers certificates related to object signing operations. OSC is issued and maintained in conformity with "Normalized Certificate Policy" defined in ETSI TS 102 042.
- TURKTRUST EV SSL Policy (2.16.792.3.0.3.1.1.5) covers certificates related to EV SSL certificates. EV SSL certificates are issued and maintained in conformity with ""Extended Validity Certificate Policy" defined in ETSI TS 102 042.

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

1.3. Participants

Participants associated with TURKTRUST certification services whose rights and obligations are described in this policy document 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, distributing and publishing certificates. TURKTRUST's issuing certification authorities operate within a hierarchy. The primary issuing certification authority has the TURKTRUST root certificate. Other issuing certification authorities who have sub-root certificates issued by this authority issue end user certificates.

According to an agreement between TURKTRUST and the Union of Turkish Bar Associations (TBA), TBA performs QEC issuance and dissemination activities towards a closed user group comprised of lawyers or judges, prosecutors and all other officials working in Turkish Judiciary according to the TURKTRUST CP and CPS documents and a service agreement, through TBA sub-root that is connected to the TURKTRUST root certificate.

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 TURKTRUST center in response to certificate requests arriving from TURKTRUST sales representatives as well as by registration centers affiliated with TURKTRUST. In both cases, certificate requests are relayed to the TURKTRUST's issuing certification authority and the certificates are issued.

1.3.3. Subscribers

Subscribers are persons whose issued certificates are based on their verified identity or name.

Verification of identity or name is performed in accordance with the relevant legislation and standards as regards to the type of certificate application. Consequences due to the use of a certificate and liability of the subscriber are qualified by the relevant legislation and subscriber's commitment or agreement.

1.3.4. Relying Parties

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

TURKTRUST's disclaimer to the relying parties against the use of certificates issued by TURKRTUST is stated in this CPS.

1.3.5. Other Participants

All certification services within the scope of TURKTRUST certification services such as certificate issuing, publication of repository and similar services are provided by TURKTRUST.

As regards to its certificate services, in order to guarantee that service shall be reliable and proper, and any private or confidential information shall not be disclosed about processes or subscribers, TURKTRUST signs a contract with a cooperating and service providing participant.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Usages

TURKTRUST's root and sub-root certificates shall be used only to sign certificates in line with the purposes of use.

TURKTRUST's QEC 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 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.

SSL and EV certificates can be used by the subscribers only for the server name in the certificate and for SSL operations.

OSC can be used by the subscriber or others who develop software under the subscriber's authority.

1.4.2. Prohibited Certificate Usage

TURKTRUST QEC cannot be used other than designated conditions in the regulations.

Use of other TURKTRUST certificates beyond the control of the subscriber is disallowed. TURKTRUST certificates cannot be used outside the limits and scope declared in this CP and CPS document.

1.5. Policy Administration

TURKTRUST, as the authority that lays down the certificate policy, is responsible for administering and registering the CP document.

1.5.1. Organization Administering the CP Document

All rights and responsibilities associated with this CP document fall with TURKTRUST.

1.5.2. Contact Person

Contact information for this CP document is as provided below:

TURKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
Address : Hollanda Caddesi 696.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. Person Determining CP Suitability for the Policy

TURKTRUST's senior management determines the suitability and applicability of this CP document.

1.5.4. CP Approval Procedure

CP document is approved by the board of management of TURKTRUST. CP so approved shall be used to regulate the policies and rules related with the CA activities.

TURKTRUST conforms to the current version of "Guidelines for the Issuance and Management of Extended Validation Certificates" which is published by CA/Browser Forum at http://www.cabforum.org for EV SSL certificates. In case of any inconsistency between the Guidelines and this CP and CPS, the Guidelines shall prevail.

1.6. Acronyms and Definitions

1.6.1. Acronyms

BR : CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

CA : Certification Authority (Electronic Certification Service Provider)

CP : Certification Policy

CPS : Certification Practice Statement

CRL : Certificate Revocation Policy

CSR : Certificate Signing Request

DN : Distinguished Name

DNS : Domain Name System

DRC : Disaster Recovery System

ETSI : European Telecommunication Standards Institute

EV : Extended Validation

IETF : Internet Engineering Task Force

OCSP : On-line Certificate Status Protocol

OID : Object Identifier

OSC : Object Signing Certificate

PKI : Public Key Infrastructure

PTC-BR: Publicly-Trusted Certificate - Baseline Requirements

QEC : Qualified Electronic Certificate

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

SAN : Subject Alternative Name

SSL : Secure Sockets Layer

TBA : Turkish Bar Associations

TCKN : Republic of Turkey the Number of Citizenship.

TSE : Turkish Standards Institution

1.6.2. Definitions

Activation: An alternative and secure method to the printing and sending a PIN envelope to the subscriber. In this method, subscriber is required to use software by TURKTRUST to "activate" his/her smart card. In order to achieve this, he/she needs to push the button for requesting the "activation code" while the smart card is plugged into the computer. The activation code is sent via SMS which enables him/her to set the PIN value.

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 standards and to find out possible errors, deficiencies, corruptions and/or abuses and impose sanctions as provided by the legislation or standards.

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

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 Signing Request (CSR): A certificate request generated by the applicant that is signed by his own private key. Generally generated in PKCS#10 formats.

Certification Authority: A public agency or institution or natural or legal persons in private law authorized 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 the Turkish Information and Communication Technologies Authority.

Directory: An electronic storage which includes valid certificates.

Distinguished Name (DN) Field: DN consists of either the subscriber's or the issuer's name. DN may comprise of different subfields like CN, O, OU, T, L and SERIALNUMBER, each of which may exist with the relaxant data depending the type of certificate.

Electronic Certificate: Electronic record that associates the public key and identity information of the subject in PKI by using the private key of the Certification Authority.

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.

EV SSL Certificate: The SSL certificate issued and maintained in accordance with the "Extended Validity Certificate Policy" defined in ETSI TS 102 042 standard.

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

Institution: The Information and Communication Technologies 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.

Mobile Operator: The operator which is the corporate applicant for the QECs that will be used for mobile signature purposes and enables the mobile signature user QEC owners to make transactions via the GSM infrastructure.

Mobile Signature: The secure electronic signature generated by the QEC owner by mobile communication devices using the related network and service infrastructure.

Mobil Signature Service: The service that conforms to the Law and the related legislation and is offered for signatures to be used by users in several services via mobile communication devices.

Object Signing Certificate (OSC): The certificate that verifies the owner of the source code of software that can be executed on a computer.

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.

Personal Identification Number (PIN): Data used by the subscriber to use the private key, protected by PIN in a secured environment.

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: Cryptographic key disclosed to the others in a public key encryption scheme; named as signature verification data in the Law.

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.

Publicly-Trusted Certificate (PTC): A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

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 the Turkish Information and Communication Technologies 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: 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.

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.

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.

SIM Card: The SIM card which hosts various specific applications, works integrated with mobile communication devices, can be used in mobile signature service and subscribers may get from mobile operators.

SSL (Secure Sockets Layer): A security protocol developed with the purpose of providing data security in internet communications, verifying the server source that serves the data and optionally verifying the client that receives the data.

SSL Certificate: The certificate that verifies the identity of the server which serves the data.

Subject: A person or a server name to appear in the CN field of a certificate.

Subscriber: The person on whose behalf a subscriber agreement or a letter of commitment setting the terms and conditions of certificate services is signed with the CA.

Sub-root 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: 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.

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.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

TURKTRUST 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

TURKTRUST ensures accuracy and up to dateness of all data kept in the repository. TURKTRUST 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 TURKTRUST 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 and CA commitments or agreements, customer guides regarding certification processes are kept public in the repository. Further, all root and sub-root certificates relating to TURKTRUST'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 TURKTRUST are kept public only if the subscribers consent in writing.

The information referred to in this section is kept publicly at the TURKTRUST's web site http://www.turktrust.com.tr.

2.3. Time or Frequency of Publication

As new versions of the documents referred in Section 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. CRL is published twice a day within 12 (twelve) hour intervals with a validity period of 24 (twenty four) hours.

TURKTRUST operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of less than ten seconds under normal operating conditions.

2.4. Access Control on Repositories

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

3. IDENTIFICATION AND AUTHENTICATION

TURKTRUST 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 TURKTRUST 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.

3.1.3. Anonymity or Pseudonymity of Subscribers

TURKTRUST does not issue QECs 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

Certificates issued by TURKTRUST allow unique identification of subscribers with information contained in DN. For legislative reasons, DN data may vary according to the type of the certificate.

3.1.5.1. QEC

The names used in TURKTRUST QECs are uniqueness among themselves.

3.1.5.2. SSL and EV SSL (Commercial Entities Resident in Turkey)

In order to distinguish the subscriber uniquely, DN in TURKTRUST SSL and EV SSL certificates are conditioned according to the type of the legal entity.

3.1.5.3. SSL and EV SSL (Commercial Entities Not Resident in Turkey)

DN in SSL certificates for entities who are not resident in Turkey are conditioned in as similar manner as in Turkish residents with the exception that any required official record or document is replaced by a local equivalent.

3.1.5.4. OSC

DN in TURKTRUST OSC is the field where personal or corporate information is found.

3.1.6. Recognition, Authentication and Role of Trademarks

Subscribers are held responsible for their trademarks appear correctly and rightfully in a certificate application. In this regard, subscribers shall be liable against any violation of intellectual property rights (IPR) of others. TURKRTUST is not only irresponsible for checking an issue for IPR in an application but is also detached from any disputes that may arise. Notwithstanding this clause, TURKTRUST holds right to deny an application or suspend or revoke a certificate if a violation of IPR is detected in the certificate application.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

It shall be verified that a certificate applicant possesses the private key. In cases where the private key is generated by TURKTRUST, this condition does not apply.

3.2.2. Authentication of Organization Identity

In cases where a certificate contains the name of a legal entity, the name of a legal entity shall be verified according to the certificate type pursuant to the following policies and rules.

3.2.2.1. QEC, SSL or OSC

The name of legal entity is verified against the official documents of the country of residence of the applicant. Verification herein is executed according to the TURKTRUST procedures.

For SSL and OSC applications, the e-mail address submitted by the authorized person who conducts the application operations on behalf of the subscriber should be verified.

3.2.2.2. EV SSL

In verification of an EV SSL application, minimum criteria to be met are as follows:

- The name of legal entity is verified against the official documents of the country of residence of the applicant. Additional to this verification, circular of signature or an equivalent official document in applicable legislation, showing the authority of the applicant to act on behalf of the legal entity is required.
- Operational existence of the legal entity is confirmed via a third party, who is a buyer of a product or service of the legal entity. Where possible, an official document, obtained from a public agency or a legally authorized person to do so, proving the operational existence suffices to verify.
- Address of the legal entity's place of business is verified according to the legal documents of the country of residence. Moreover, telephone numbers, submitted by the applicant, are checked if they are exactly matched with the official records. In case of mismatch, correction is required. Verified telephone is the called for applicant to confirm the application.
- The e-mail address submitted by the authorized person who conducts the application operations on behalf of the subscriber should be verified.
- The following conditions should be met as well:
    - The legal entity is the owner of the DNS registry, or
    - The legal entity is given the exclusive right and authority to use the DNS name.

All conditions that apply for authentication of legal entity for an EV SSL applicant are given in Appendix of CPS document. Given the conditions here, the process of authentication of legal persons is conducted according to the TURKTRUST procedures.

3.2.3. Authentication of Individual Identity

Personal information for persons applying for qualified electronic certificates shall 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 second and subsequent applications, face to face authentication turns into a must if either of the following is the case:

In cases where

- It passes more than 6 (six) months after the expiry date of the last certificate of the subscriber.
- TCKN or name in DN field in the last certificate of the subscriber is about to change.

In all other cases, telephone, fax messages or e-mail are possible ways of authentication in line with the TURKTRUST procedures.

3.2.4. Non-verified Subscriber Information

The e-mail addresses in QEC applications are accepted upon the declaration of the applicant and contained in the certificate without further verification.

Such other fields as "S", and "O" that may appear in DN field of a certificate are also accepted upon the declaration of the applicant as factual information.

3.2.5. Validation of Authority

In cases where the name of a legal entity is to be contained in a certificate, the applicant must submit an official document showing the authority of the applicant to act on behalf of the legal entity.

3.2.6. Criteria for Interoperation

Cross or unilateral certification with another electronic certificate service provider for easing interoperability is not applicable.

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. New certificate application can also be done in electronic media and by signing with the private key attached to the current certificate while the last certificate is still valid. In such a case, if the key pair is generated by the subscriber, the public key is transmitted to the CA along with the certificate request.

If any of the data to be contained in the new certificate is about to change, then such change must be based on the official documentation. Change in other subscriber's data, not to be contained in the certificate, is accepted upon the written or electronic declaration of the applicant.

In re-keying, face to face verification for QEC is not pursued. However, in cases where telephone calls or fax messages lead to indecisiveness, face to face verification is then required.

A re-key request for a valid subscriber of QEC cannot be called before 30 (thirty) days prior to the date of expiry of the certificate. A live request lasts for 30 (thirty) days.

For SSL, EV SSL and OSC, renewal and rekey is not performed.

The applicant shall be properly informed if a change in terms and conditions of TURKTRUST services has occurred in the period between the initial identity verification and the time of rekey request of the applicant.

3.3.2. Identification and Authentication for Re-key after Revocation

Except the following reasons of revocation, authentication for re-key after revocation is performed as explained in Section 3.3.1:

- Reasons due to incorrect, fault or incomplete data in the certificate.
- Reasons due to incorrect, fault or incomplete data in documentation proving authority, address or else, or complete invalidation of such documentation.
- Reasons due to fact that operational or legal existence of the subscriber ceases or due to strong suspicion that any such event occurs.

Re-key is not applied for the conditions stated here and certificate application procedures are carried out as if an application for the first time is done.

3.4. Identification and Authentication for Revocation Request

TURKTRUST receives QEC revocation requests in secure ways as described below and performs authentication:

- Subscriber, by using credentials given to him at the application phase, authenticates himself on the web, interactive voice response (IVR) or other TURKTRUST software to suspend or revoke his certificate.
- Subscriber may send revocation request by a fax message. In that case, the certificate is immediately suspended. With the submission of the revocation request in writing or at the end of the period of suspension, the certificate is revoked. In the period of suspension, the suspension status is removed if the subscriber declares in writing that reasons of revocation no longer exist.

TURKTRUST receives revocation requests for SSL, EV SSL and OSC in secure ways as described below and performs authentication:

- Subscriber may send revocation request by a fax message with signature of authorized person. Upon receiving this fax message authorities are contacted by phone to verify this revocation request. After verifying this request the certificate is revoked.
- If subscriber prefers to revoke the certificate on the web, the server administrator connects to interactive certificate operations in the TURKTRUST web page by entering certificate type, serial number and similar data. After completing the secondary identity verification, revocation reason is then entered into the system. Online revocation transaction will be completed in accordance with 7 days 24 hour principle. The authorized person will be informed of the transaction result via email.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

TURKTRUST generates certificates and manage the certificate life-cycle in accordance with the policies and rules set forth in this CP. In what follows, principles conducted per certificate type are described.

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application?

Any real person free of any legal obstacles may apply for QEC or OSC.

For SSL, EV SSL and OSC, including private legal entities and public entities, any legal entity may apply for a certificate.

Hereby TURKTRUST declares its right to retain and archive all the necessary information that shall be submitted during a certificate application for a period of 20 (twenty) years.

4.1.2. Enrollment Process and Responsibilities

Enrollment of a certificate application is composed of two main steps as described below:

- Certificate enrollment: Certificate application is verified against the documentation and enrolled completely and free of errors.
- Key generation: Public and private key pairs are generated either by TURKTRUST or the applicant. In case of a key generation by the applicant, the applicant shall send public key to TURKTRUST in electronic form as stated in standards and TURKTRUST procedures. In this case, TURKTRUST verifies this electronic form whether it proves the possession of the private key of the applicant.

Practicing these steps with respect to different types of certificates is described in detail below.

TURKTRUST QEC application can be realized with different methods. For places where TURKTRUST has a local office, applicant may show up at the office or may request on-site application at his own location upon additional payment. For places where no local TURKTRUST office exists, applicant must make face to face authentication at a notary. All TURKTRUST QEC applications can be initiated online at TURKTRUST web site. For applications of the type exprEss-Sign (where the certificate is issued on the same or the next day of request), online application is prerequisite. In a QEC application, the applicant fills in the application form thoroughly and signs. The applicant then sends to TURKTRUST the application form, the Letter of Commitment signed by the subscriber and the attached documents of authentication. In exprEss-Sign applications, the application documents are hand delivered and authentication is performed. QEC applications aimed at use of mobile signature are made by the mobile operator on behalf of the subscriber. Mobile operator acts as if its subscribers are part of its corporate, and thus collects all the required information and documentation and submits to TURKTRUST.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

When processing a QEC application, the identification of the applicant shall be authenticated based on official documents pursuant to the laws. At the initial identity verification, the authentication action is made face to face by TURKTRUST. This may not be required in subsequent applications.

QEC applications aimed at use of mobile signature are initiated by a pre-registration on channels provided by the mobile operator. Subsequently, subscriber's information and documentation are obtained via registration offices of the mobile operator. SSL, EV SSL and OSC applications are carried out according to the principals of Section 3.2 and relevant TURKTRUST procedures.

4.2.2. Approval or Rejection of Certificate Applications

Based on the following conditions, a certificate application is approved:

- According to the principals of Section 3.2 and relevant TURKTRUST procedures, required forms and documentation are completed.
- Payment is made.

Occurrence of any of following conditions leads to the rejection of the application:

- According to the principals of Section 3.2 and relevant TURKTRUST procedures, required forms and documentation are not completed.
- Applicant is not responding timely or satisfactorily to the questions raised for verifying the submitted information and documentation.
- In 30 (thirty days) after the enrollment of an SSL, EV SSL or OSC application, CSR is not delivered to TURKTRUST.
- For an SSL, EV SSL or OSC application, there emerges a strong opinion that issuing the certificate may damage TURKTRUST reputation.
- Payment is not made.

4.2.3. Time to Process Certificate Applications

QEC applications delivered to TURKTRUST are processed within at most 5 (five) working days. TURKTRUST exprEss-Sign applications are processed on the same day.

SSL, EV SSL or OSC applications delivered to TURKTRUST are processed within at most 5 (five) working days.

Times given in this section is applicable only if certificate applications are accurate and free of errors, and conform with the principles of Section 3.2 and TURKTRUST procedures.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

Accepted certificate applications with regard to the principles stated in Section 4.2.2. are processed as described in TURKTRUST procedures at TURKTRUST certificate production centers.

4.3.2. Notification to Subscriber of Issuance of Certificate

After certificate issuing is completed, the subscriber is informed by e-mail or SMS message.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are under obligation to review and verify the accuracy of the data in all certificate types before installing or using the certificate and to notify TURKTRUST and request revocation of certificates which happen to include data that are inaccurate or inconsistent with the certificate applications.

4.4.2. Publication of the Certificate by the CA

Certificates are published in the web or directory servers upon subscribers' consent in writing.

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

A subscriber should use his certificate and his private key related to his certificate in accordance with the Law, the Ordinance and other regulatory actions, and stipulations indicated in the CP and CPS documents and the related subscriber's agreement or letters of commitment.

A subscriber is under obligation for protecting the private key related to his certificate against third party access and using the certificate within the scope and authority defined in the legal regulations, CP and CPS documents and the related subscriber's agreements or letters of commitment.

For QEC, the private key activation data is sent to the subscriber by password envelope in those circumstances when activation operation is not used. Subscriber determines the activation data through the software supplied by TURKTRUST in case activation is applied instead of password envelope. QEC owner should:

- Receive in person the secure electronic signature creation device and the relevant activation data, if exists, issued to his name.
- Not allow other people to use his mobile phone and e-mail address for those circumstances when code activation is used.
- Immediately inform the CA for certificate revocation 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..

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties 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 Ordinance and other regulatory actions, and the CP and CPS documents.

Certificate validity control should be done under secure and appropriate conditions. Relying parties take necessary precautions if there is any doubt about an adverse situation. In this respect, before relying on a certificate, relying parties should check:

- Whether the certificate is used in accordance with its usage purpose, in particular the certificate is not installed on systems such as nuclear facilities, air traffic

control, aircraft navigation or weapons control systems where an operational failure may lead to injury, death, or environmental damage.

- Whether the "key usage" field is in accordance with the usage condition of the certificate,
- That the root and sub-root certificates that the certificate is based on are valid, i.e. the root and sub-root certificates neither suspended nor revoked nor expired, and that he recognizes the CA.

Relying parties are under obligation to use secure software and hardware defined by legislation and standards during these operations.

TURKTRUST cannot be held responsible for relying parties not fulfilling the conditions stated here about public key and certificate usage before relying on the certificate.

4.6. Certificate Renewal

Certificate renewal is made by issuing a new certificate where the validity period is extended provided that the information in the certificate remains the same including the public key as well.

In order for a certificate to be renewed, the private key of the certificate should not have been compromised.

According to the certificate types, differences in certificate renewal are as follows:

For QEC, renewal application cannot be made based on certificates that are expired. With respect to the cryptographic security of the key pair, the total validity period of a certificate shall not exceed 3 (three) years.

4.6.1. Circumstances for Certificate Renewal

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

An expired certificate may also be renewed provided that the renewal request is done within the validity period of the certificate. This renewal operation is done within at most 30 (thirty) days, otherwise the certificate renewal request is rejected.

4.6.2. Who May Request Renewal

The subscriber or a person who is authorized to represent the subscriber may request renewal.

4.6.3. Processing Certificate Renewal Requests

Certificate renewal is only performed for QEC. As explained above, in circumstances where the private key is compromised or the cryptographic security of keys is to be lost along with the renewal period or the 30 (thirty) day validity period of renewal request expires, the renewal request is rejected.

For QEC, the certificate renewal period is 1 (year) in all cases. Within the validity period, the QEC owner may request renewal via internet by using electronic signature. In this operation, the subscriber signs the renewal request, as well as that demonstrates possession of the private key based on the certificate. Acceptance of the renewal request depends on satisfying all the conditions below:

- A written commitment is taken from the subscriber indicating explicitly that the information given during the previous application is still valid. In case this

written commitment is not made available or knowledge of a change in the certificate information is received, then principles of Section 4.7 apply.

- Along with the renewed certificate, the total validity period of the keys shall not exceed 3 (three) years. In case of any indication about compromise of subject's private key, re-key is required.
- Payment is made.

4.6.4. Notification of Renewed Certificate Issuance to Subscriber

Policies of Section 4.3.2 apply.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Policies of Section 4.4.1 apply.

4.6.6. Publication of the Renewal Certificate by the CA

Policies of Section 4.4.2 apply.

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

Not applicable.

4.7. Certificate Re-key

Except for the special condition mentioned below for QEC, certificate re-key is not applicable.

4.7.1. Circumstances for Certificate Re-key

For QEC in the first 3 (three) months of the validity period, a new certificate is issued with re-key without any new documentation of verification if the certificate is erased from the smart card, or the card is lost, or the card malfunctions. The data submitted at the certificate application remains unchanged is prerequisite. In cases where deemed necessary, data remains unchanged shall be checked.

4.7.2. Who May Request Certificate Re-keying

A real person may request re-key for a QEC.

4.7.3. Processing Certificate Re-keying Requests

In case of any indication or doubt about any change in any information in the QEC, related information and supporting documents are taken again.

4.7.4. Notification of New Certificate Issuance to Subscriber

Policies of Section 4.3.2 apply.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

Policies of Section 4.4.1 apply.

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

Policies of Section 4.4.2 apply.

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

Not applicable.

4.8. Certificate Modification

4.8.1. Circumstances for 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.

New certificate application is performed according to the policies stated in Section 4.1.

4.8.2. Who May Request Certificate Modification

Policies of Section 4.1.1 apply.

4.8.3. Processing Certificate Modification Requests

Policies of Section 3.2 apply.

4.8.4. Notification of New Certificate Issuance to Subscriber

Policies of Section 4.3.2 apply.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Policies of Section 4.4.1 apply.

4.8.6. Publication of the Modified Certificate by the CA

Policies of Section 4.4.2 apply.

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

4.9.1.1. Subscriber Certificates

Where a certificate loses its validity within the term of use, it shall be revoked. Upon receiving the revocation request for QEC revocation process is completed immediately; for SSL, EV SSL and OSC revocation process is completed within 24 (twenty four) hours. Suspension process is not applied for SSL, EV SSL and OSC. The following circumstances shall require revocation of a certificate:

- Request by the subscriber or the person authorized to represent,
- It is understood that the information regarding a qualified electronic certificate or an application is false or incorrect; TURKTRUST may have the opinion that this requirement may pose plausible evidence. Both the subscriber and the person authorized to represent have this opinion as well.
- For QEC, after exprEss-Sign certificate generation, if the e-signature package that is to be delivered through the related registration authority is not taken by the subscriber within 1 (one) month, or after standard QEC generation, if the e-signature package delivered by courier is not taken by the subscriber within 1 (one) month,
- A change occurs in the information regarding the subject or subscriber included in a certificate's content

- It is learned that the subscriber's legal capacity is restricted, or the subscriber is bankrupt or lost in danger of death, or died,
- It is understood that or a notification is received indicating legal existence or business activity of the legal person subscriber has been terminated for SSL and EV SSL certificates,
- It is understood or evidence found that the certificate was misused,
- It is understood that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name,
- It is discovered that the SSL certificate is being used to enable criminal activities such as phishing attacks, fraud or the distribution of malware,
- The private key has been lost, stolen, disclosed or a risk of access or use by a third party arises,
- The subscriber has lost his/her control over the private key due to the compromise of activation data or similar reasons,
- The software or hardware in which the private key is located has been lost, broken down or compromised,
- It is understood that or a notification is received indicating the certificate has been used in contradiction to the provisions of the CP and CPS guide documents and TURKTRUST Certificate Subscriber's Agreement or Letter of Commitment,
- It is understood or received a notification that a court or an authorized person has received the authorization of use of subscriber's domain name for SSL and EV SSL certificates,
- The GSM subscriptions of QEC subscribers who use mobile signature have been terminated by the GSM operator,
- TURKTRUST, in its sole discretion, detects any irregularity while issuing the certificate on the merits of the application of this CPS document,
- The disappearance of the right to give the certificate based on Law for QECs,
- The disappearance of the right to give the certificate of TURKTRUST for EV SSL certificates,
- Any of the algorithms, or associated parameters, used by TURKTRUST or its subscribers are compromised or become insufficient for its remaining intended usage,
- The private keys of TURKTRUST's sub-root and root certificates are out of suspicion or compromised,
- TURKTRUST suspends provision of certification services or has not made arrangements for another CA to provide revocation support for the certificate.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties,

4.9.1.2. TURKTRUST's Sub-root Certificates

Where a su-root CA certificate loses its validity within the term of use, it shall be revoked within 7 (seven) days. The following circumstances shall require revocation of a certificate:

- TURKTRUST obtains evidence that the sub-root private key corresponding to the public key in the certificate suffered a key compromise,
- TURKTRUST obtains evidence that the certificate was misused,
- TURKTRUST is made aware that the certificate was not issued in accordance with the BR or the applicable Certificate Policy or Certification Practice Statement documents,
- TURKTRUST determines that any of the information appearing in the certificate is inaccurate or misleading,
- TURKTRUST ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate,
- TURKTRUST's right to issue certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository,
- Revocation is required by TURKTRUST's Certificate Policy and/or Certification Practice Statement,
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.1.3. Subordinate CA Certificate

Where a subordinate CA certificate loses its validity within the term of use, it shall be revoked within 7 (seven) days. The following circumstances shall require revocation of a certificate:

- The Subordinate CA requests revocation in writing,
- The Subordinate CA notifies TURKTRUST that the original certificate request was not authorized and does not retroactively grant authorization,
- TURKTRUST obtains evidence that the Subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise,
- TURKTRUST obtains evidence that the certificate was misused,
- TURKTRUST is made aware that the certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement,
- TURKTRUST determines that any of the information appearing in the certificate is inaccurate or misleading,
- TURKTRUST or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate,
- TURKTRUST's or Subordinate CA's right to issue certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository,
- Revocation is required by TURKTRUST's Certificate Policy and/or Certification Practice Statement,

- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2. Who Can Request Revocation

The following people may request revocation:

- The subscriber himself, or the legal entity authorized to represent the subscriber juristic people if there exists a corporate expression in the certificate for QECs and OSCs,
- Secure electronic signature creation device owner for QECs,
- The legal entity authorized to represent the legal person subscriber for SSL and EV SSL certificates and OSCs,
- Mobile operator for QECs used for mobile signature,
- Subordinate CA's authorized persons, for the certificates that are issued by Subordinate CA,
- TURKTRUST's authorized persons (TURKTRUST center and registration authorities) for end user certificates and root and sub-root certificates where security concerns necessitate.

4.9.3. Procedure for Revocation Request

Revocation requests for QECs shall be received in different ways as follows:

- Via TURKTRUST web site, on 7 days 24 hours basis,
- Via the Interactive Voice Response (IVR) system over the telephone number announced to all customers and published openly, on 7 days 24 hours basis,
- Via a declarative statement written by the subscriber (signed papers sent by fax or by post), within official working hours.

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

For revocation of QECs used for mobile signature, the subscriber notifies revocation request by contacting with mobile operator call center. Revocation status after the completion of process is notified to the subscriber via mobile signature service infrastructure.

If there exists a corporate expression in the certificate, revocation requests for QECs may be obtained from the subscribers as well as from the authorized persons representing the related corporation of companies along the approved revocation applications. The revocation status after the action shall be notified by e-mail to the subscriber and organizational authorized personnel.

In circumstances where QECs used for mobile signature shall be revoked by the mobile operator, revocation request is sent to TURKTRUST via mobile signature service infrastructure.

Revocation requests for SSL, EV SSL and OSCs are taken either TURKTRUST web site on 7 days 24 hours basis or with a revocation request letter signed by the authorized person to act on behalf of the legal entity. The revocation status after the action is notified by e-mail to the authorized personnel.

If and when subscriber prefers to revoke the certificate via TURKTRUST web site, the server administrator connects to interactive certificate operations in the TURKTRUST web page by entering certificate type, serial number and similar data. After completing the secondary authentication stage, revocation reason is entered into the system. Online

revocation transaction will be completed in accordance with 7 days 24 hours basis. The revocation status after the action shall be notified by e-mail to the subscriber and organizational authorized personnel.

Where a security compromise occurs at TURKTRUST, or a notice is received regarding the existing certificates or a fault is detected in TURKTRUST's internal operation, TURKTRUST may initiate certificate revocation. For all certificate revocations originating from TURKTRUST, the outcome shall be notified by e-mail to certificate users. Where necessary, new certificate issuing operations shall be immediately started after the revocation without demanding any fee.

There is neither a procedure for reinstating a revoked certificate nor a tool made available to anyone to reinstate a revoked certificate. Revocation transaction leads to several updates in the database; the immediate update of OCSP service and next update of CRL. A revoked certificate shall continue to be in CRL until the certificate expires.

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

4.9.4. Revocation Request Grace Period

As long as the technical and commercial opportunities allowed, the certificate revocation request is processed within the shortest period of time.

4.9.5. Time within which TURKTRUST Must Process the Revocation Request

TURKTRUST immediately resolves all certificate revocation requests transmitted over the web and received through telephone (IVR) 7 days and 24 hours, following the approval of the request and authentication of identity. Revocation requests transmitted on paper shall be taken into evaluation in the shortest time possible during working hours and necessary actions shall be completed urgently.

The revocation requests for QECs used for mobile signature are sent to TURKTRUST via mobile signature service infrastructure following necessary authentication carried out by the mobile operator that is the corporate applicant itself and revocation requests are immediately resolved.

4.9.6. Revocation Checking Requirements for Relying Parties

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

4.9.7. Certificate Revocation Lists (CRL) Issuance Frequency

TURKTRUST 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 TURKTRUST sub-root certificates are issued at least once a year or upon sub-root certificate 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)

TURKTRUST 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, the status of certificates may be inquire on-line by appropriate software on the customer side. It is possible by this inquiry to obtain information about the status of a certificate at any specific time (valid, suspended, revoked, expired/unknown).

Within the scope of TURKTRUST OCSP service, the responses sent to the client systems are signed using the OCSP responder certificates that are generated for the purpose of signing OCSP responses. Any response for a certificate issued by TURKTRUST is signed using an OCSP responder certificate that is issued by the root or sub root certificate that issued the queried certificate.

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

TURKTRUST 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 TURKTRUST, end user certificates affected by the incident shall be revoked by TURKTRUST. If the root or sub-root certificates of TURKTRUST need to be revoked, end user certificates that have the signature of such certificates shall also be revoked and subscribers shall be informed.

The compromise incident and its effects shall be notified by TURKTRUST to subscribers and relying parties urgently over the public website and where necessary via the press media.

In case of a CA compromise notification, subscribers shall no longer be allowed to use their certificate.

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

4.9.13. Circumstances for Suspension

Where the source of a QEC revocation request could not be verified, TURKTRUST 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.

Suspension is not applicable for SSL, EV SSL and OSC. After completing the secondary identity verification, revocation process is completed.

4.9.14. Who Can Request Suspension

Policies of Section 4.9.2 apply.

4.9.15. Procedure for Certificate Suspension

Policies of Section 4.9.3 apply except for the situations defined below:

Where a security compromise occurs at TURKTRUST, or a notice is received regarding for existingQEC, TURKTRUST may suspend relevant certificates until the

revocation requirement is validated. A certificate suspension process initiated by TURKTRUST may originate from registration authorities or issuing certification authorities. For all certificate suspensions originating from TURKTRUST, the outcome shall be notified to certificate users.

Where a security compromise occurs at TURKTRUST, or a notice is received regarding for existing SSL, EV SSL and OSC are immediately revoked after completion of the secondary authentication stage, then the related subscribers are notified of the result by email.

TURKTRUST's root and sub-root certificates shall not be suspended.

4.9.16. Limits on Suspension Period

QECs suspended by TURKTRUST, 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. Certificate, suspended where the subscriber is not sure whether any circumstance that requires revocation exists, shall be revoked when the subscriber reconfirms the request 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 QECsare suspension that there is no circumstance that requires revocation, such certificates may be taken out of suspension and moved into the valid status.

The suspension process is not applicable for SSL, EV SSL and OSC.

4.10. Certificate Status Services

Certificates issued by TURKTRUST shall be published over the web accessible to all subscribers and relying parties provided that subscribers consent in writing. Certificates may be published in a manner accessible directly on the web or via 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

TURKTRUST publishes CRL twice a day within 12 (twelve) hour intervals with a validity period of 24 (twentyfour) hours even if there is no change in the status of certificates.

TURKTRUST 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

TURKTRUST provides CRL and OCSP services under conditions stated in Section 4.10.1 without interruption 7 days 24 hours. TURKTRUST certificate services given from the Headquarters are always sustained with sufficient level of infrastructure for availability and fail over purposes. In case where a situation beyond the control of TURKTRUST arises that leads to interruption of services, TURKTRUST DRC shall take over the management of certificate services not later than 2 hours of the situation.

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

In case private key is generated by TURKTRUST itself, TURKTRUST does absolutely not store or re-generate these data. Moreover, TURKTRUST does not hold any data it could re-generate it.

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 CP document covers non-technical security controls that TURKTRUST practices to ensure facility and operation safety when performing certification services.

5.1. Physical Controls

5.1.1. Site Location and Construction

The TURKTRUST 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 TURKTRUST and TBA centers are constantly controlled.

5.1.3. Power and Air Conditioning

Uninterrupted power supplies have been installed to operate all hardware and equipment used at the TURKTRUST center. Particularly in areas where computer hardware is concentrated, adequate and uninterrupted ventilation is provided.

5.1.4. Water Exposures

TURKTRUST center is protected against floods and water exposures.

5.1.5. Fire Prevention and Protection

Fire alarm systems and fire extinguishing systems providing an immediate intervention to the probable fires have been installed in the TURKTRUST building.

5.1.6. Media Storage

Backups of all records generated during the activities of TURKTRUST are kept in appropriate storage media.

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 TURKTRUST units shall be removed appropriately out of the facility.

5.1.8. Off-site Backup

TURKTRUST, 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 TURKTRUST:

- **Executive Managers:** Managers technically and administratively responsible for running TURKTRUST's CA services.
- **Registration and Customer Services Officers:** Employees responsible for routine certification services such as customer services, document control, processes relating to certificate registration, generation, suspension and revocation.
- **Security Officers:** Employees responsible for administering the implementation of the security policies and practices.
- **System Administrators:** Employees authorized to install, configure and maintain CA systems and also authorized to perform system backup and recovery.
- **System Auditors**: Employees authorized to view archives and audit logs of CA systems.
- **Security Personnel:** Serving as security personnel who are responsible of physical security of the entire TURKTRUST facilities.

5.2.2. Number of Persons Required per Task

A multi-person controlled system has been established at TURKTRUST 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, revocation and backup operations relating to TURKTRUST root and sub-root 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 TURKTRUST 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 TURKTRUST 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

TURKTRUST assesses in detail personal backgrounds and references of personnel employed at TURKTRUST, 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

TURKTRUST'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.

5.3.5. Job Rotation Frequency and Sequence

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

TURKTRUST 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, TURKTRUST signs a service contract with the contractor company. This service contract stipulates the security clauses and service principles required by TURKTRUST.

5.3.8. Documentation Supplied to Personnel

TURKTRUST's personnel are supplied with the CP and CPS documents, operational and security procedures and instructions relating to certification processes, job descriptions 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 are kept by TURKTRUST. 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 TURKTRUST units having trusted roles, employees' entry and exit records to/from TURKTRUST 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, date and time of the operation and result of the action are 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 TURKTRUST'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 the related 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 TURKTRUST's operation, all audit logs stated in Section 5.4, applications, requests and instructions relating to certification processes, all supporting documents obtained on paper and subscriber's agreement (or letter of commitment), 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 TURKTRUST 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 TURKTRUST's operation regarding QECs shall be retained for at least 20 (twenty) years. Archives regarding SSL's, EV SSL's and OSC's shall also be retained for 20 (twenty) years by TURKTRUST.

5.5.3. Protection of Archive

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

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements for Time-Stamping of Records

All electronic archive records are kept by TURKTRUST bundled with time data.

5.5.6. Archive Collection System

Archive logs are collected using the TURKTRUST archive management system according to the related procedures.

5.5.7. Procedures to Obtain and Verify Archive Information

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

5.6. Key Changeover

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

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Where events or security compromises occur which would prevent TURKTRUST's operations, intervention is made pursuant to TURKTRUST'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 TURKTRUST private keys are compromised, the relevant certificates shall be revoked pursuant to TURKTRUST's disaster management procedures and business continuity plans and new private keys shall be generated and enabled pursuant to Section 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

TURKTRUST has established a disaster recovery center (DRC) outside the Headquarters. Data stored at TURKTRUST Headquarters are backed up to ensure the business continuity after a disaster.

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

5.8. Termination of TURKTRUST Operations

Where TURKTRUST 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. TURKTRUST 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, TURKTRUST shall revoke relevant certificates and notify all related parties. In such case, TURKTRUST generates the last CRL log and destroys its own private key and backups.

SSL and EV SSL certificate and OSC subscribers shall be also notified. The mandatory transfer process for QEC, in principle, is tried to be performed for these certificates. In this context, within the validity period of certificates, the points related to continuity of TURKTRUST obligations and issuances of certificate status information for valid certificates are regulated in the transfer process.

6. TECHNICAL SECURITY CONTROLS

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

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pairs for TURKTRUST root and sub-root certificates are generated pursuant to the TURKTRUST procedures for key generation and dissemination for root certificates under the dual control of authorized personnel as described in Section 5.2.2 in a technically and administratively secured environment. Private keys are protected against unauthorized access by physical and technical security measures.

In all cases where TURKTRUST handles key generation, key pairs are generated in hardware security modules that have at least EAL 4+ or FIPS 140-2 Level 3 security level. The length of the key pairs and algorithms used are made to be compatible with current legislation and standards. The life of the key pair generated is limited in the same way up-to-date legislation, standards, and the lifetime of the keys with respect to cryptographic security. It is provided to continue to serve without interruption by generating a new key pair and a certificate within a suitable time margin before the validity period ends for TURKTRUST root and sub-root certificate.

TURKTRUST HSMs are kept and operated under physical and electronic protection against all types of intervention. The secure backup of the data in HSMs are taken and stored according to the procedures. Thus when an HSM completes its physical and economic lifetime, the private keys on the HSM are destroyed as described in Section 6.2.10 while keeping the relevant backups in other media to be used in new HSM devices.

QEC sub-root key generation for the Union of Turkish Bar Associations (TBA) is performed by a hardware security module in TBA's certificate production center. The generated public key is taken to TURKTRUST certificate production center in PKCS#10 standard via offline media with an electronic file that is signed by the private key and TBA's QEC sub-root is generated. The generated QEC sub-root of TBA is installed to TBA's production system so as to make it ready for signing QECs by TBA. The hardware security module which is located in TBA has the same security level as TURKTRUST's hardware security modules where TURKTRUST's other root and sub-root certificates reside.

Server administrators who apply for server certificates and technical administrators 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

The signature creation and verification data for QEC owners can be produced at TURKTRUST side or at client-side. When the production takes place in TURKTRUST side, it is performed in hardware security modules having the appropriate security level in certificate production center. In this case, the private keys that belong to subscribers are neither kept nor copied at TURKTRUST. Alternatively, an applicant having a secure electronic signature creation device can produce his/her signature creation and verification data in accordance with TURKTRUST certificate application methods.

In QEC applications aiming mobile signatures usage, the key pair is generated in the SIM card of the subscriber and signature verification data is conducted to TURKTRUST for certificate production via mobile signature service infrastructure.

QEC applicants who self-generate their key pairs are responsible for the use of a secure electronic signature creation device.

The applicants who will apply for SSL certificates, EV SSL certificates or object signing certificates are responsible for a secure key generation during application.

For a QEC whose key pair is generated by TURKTRUST, the signature creation data in a secure electronic signature creation device is delivered to its owner by courier in exchange for owner's authentication and signature. A secure electronic signature creation device access password envelope is delivered to its owner by courier in the same fashion. This delivery does not occur when activation takes place instead of password envelope.

Within the scope of "exprEss-Sign" applications, the signature creation and verification of data pairs are already produced in TURKTRUST Headquarters; the signature creation data, by default, are sent to the local offices of TURKTRUST on secure signature creation devices. After having produced, the certificate which is installed to the applicant's secure electronic signature creation device in related office is delivered to its owner (together with password envelope if exists) by a TURKTRUST authorized personnel in exchange for owner's authentication and signature.

In QEC applications aiming mobile signatures usage, the signature creation data is generated in the SIM card of the subscriber.

6.1.3. Public Key Delivery to the ECSP

Where key pair generation takes place on the certificate applicant side, the certificate request has to be signed by the private key. To prevent third parties accessing the request information, the request shall be communicated to TURKTRUST through electronic communications.

6.1.4. TURKTRUST Public Key Delivery to Relying Parties

TURKTRUST root and sub-root certificates are . Thus, relying people may use public keys of TURKTRUST.

6.1.5. Key Sizes

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

TURKTRUST's root and sub-root certificates are 2048 bit length when and if RSA keys are used.

For all end user certificates issued by TURKTRUST, 2048 bit RSA key pairs are used.

The information about digest algorithm used in certificates issued by TURKTRUST is given Section 7.1.3.

6.1.6. Key Generation and Quality Checking

Where key generation takes place at the TURKTRUST 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. However in this case,

TÜRKTRUST verifies the validity of the CSR file sent by the customer according to key length and other parameters along with the signature on the file. The system is automatically controls received CSR file and rejects if signs with weak private key.

6.1.7. Key Usage Purposes

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

Keys of root and sub-root certificates of TURKTRUST's issuing certification authorities shall be used for signing certificates and CRLs.

Keys of OCSP server certificates of TURKTRUST shall be used for signing OCSP responses.

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 TURKTRUST are realized in secure cryptographic hardware modules, i.e. HSMs, conforming to the standards specified in the Communiqué. Before using these HSM devices for the first time after procurement, controls are applied to ensure that these devices are not tampered with during shipment and while stored. Factory packaging and security seals are checked upon receiving the devices and these HSMs are stored and used in physically and technically secured working areas. During the whole life time of HSMs, the devices are kept under continuous control regarding their functionality and any possible incidents are managed according to the incident management procedure.

Where private keys of subscribers of QECs are generated on the TURKTRUST 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 sub-root certificates of issuing certification authorities under TURKTRUST. 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 TURKTRUST's private keys.

Private keys of QECs 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.

6.2.3. Private Key Escrow

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

6.2.4. Private Key Backup

Private keys of end user certificates issued by TURKTRUST are not backed up, or copied.

In order to ensure continuity of services in case of a disaster or a problem, the private keys of root and sub-root certificates of TURKTRUST's issuing certification centers are kept under physical and technical security controls with respect to TURKTRUST 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 sub-root 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 TURKTRUST 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 QECs.

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 sub-root certificates of TURKTRUST'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 QECs are generated on the TURKTRUST 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.

6.2.8. Method of Activating Private Key

Private keys of root and sub-root certificates of TURKTRUST'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 QECs shall be activated by entering password to the secure electronic signature creation device.

Private keys of SSL, EV SSL and OSCs shall be activated on the software or hardware belonging to the subscriber.

The subscriber is responsible for the unauthorized use of the activation data by other persons, taking necessary measures to prevent data theft or loss.

6.2.9. Method of Deactivating Private Key

Private keys of root and sub-root certificates of TURKTRUST'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 or time-out of the operation. 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 QECs shall be activated for a certain length of time upon password entry to the secure electronic signature creation device, and deactivated at operation time-out. 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 SSL, EV SSL and OSCs shall be deactivated on the software or hardware belonging to the subscriber.

6.2.10. Method of Destroying Private Key

All copies of the private keys of root and sub-root certificates of TURKTRUST's issuing certification authorities that reside on active HSM devices are destroyed upon expiry of the certificate only by authorized persons using the zeroization function of related HSMs and the operations performed are logged according to procedures. For this operation, at least two persons should be present.

Private keys associated with QECs and stored in the secure electronic signature creation devices could be destroyed by deletion of the key from the device or destroying the device itself.

There is no stipulation for destroying private keys of end user SSL, EV SSL certificates and OSCs upon certificate revocation or expiry. The subscriber may destroy the private key if he so wishes.

6.2.11. Cryptographic Module Rating

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

Private keys of QECs 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 sub-root certificates of TURKTRUST's issuing certification authorities are stored for 20 (twenty) years by the CA.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The term for QECs, SSL certificates and OSCs issued by TURKTRUST is 1 (one), 2 (two) or 3 (three) year(s). For the sake of cryptographic security of the key pairs, the total validity period with the same content for QECs cannot exceed 3 years.

The term for EV SSL certificates issued by TURKTRUST is 1 (one), 2 (two) year(s) or at most 27 (twenty seven) months.

The term for root and sub-root certificates of TURKTRUST'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

Activation data refers to a passphrase, password, PIN or else any private data that are used to operate private keys.

The generation of the keys belonging to TURKTRUST sub-root and root certificates and the creation of the passphrases to them is done according to the ceremony described in the Root Certification Procedure. The private keys of root and sub-root certificates of TURKTRUST's cryptographic modules in which such keys are located can be accessed by presence of two authorized persons who possess the passphrases as described in Section 6.2.2. These passphrases are forced to consist of 12 alpha-numeric characters that comply with the relevant sections of Baseline Requirements.

Biometric verification is also required besides these passwords to access the system. The creation, installation and usage of access codes, are logged with keyed hash mechanism and kept in a dedicated database.

The private key of QEC is kept secured in an integrated circuit on a smart card that complies with the relevant security standard and legislation. The private key of QEC can only be activated via PIN which can be set by the certificate owner. Before the delivery of a QEC to its owner, a six digit random PIN is generated and set to secure the private key on the smart card. A subscriber, to whom the smart card is delivered, requests the QEC activation code for replacing the random PIN on the smart card which is unknown to the subscriber with a PIN he/she determines by using the TURKTRUST smart card management software. Then the subscriber can determine his/her PIN by using the QEC activation code having been sent to his/her mobile phone via SMS again using the TURKTRUST smart card management software. The mobile phone number to be used in this QEC activation operation is submitted to TURKTRUST by the owner during the certificate application process.

In circumstances where QEC activation operation is not used, PINs for the signature creation data of QEC owners are delivered to them by password envelopes via courier service as an alternative method. Again, a six digit random PIN is generated and set to secure the private key on the smart card and written in a sealed password envelope.

TURKTRUST strongly recommends the security items listed below to subscribers of QEC while creating their access passwords:

- At least 6 (six) character long,
- A character in it should not be repeated,
- Not to use birth date, name and can be easily guessed data

TURKTRUST recommends to change the activation data at least once in 6 (six) months and determine a new activation data other than the predecessor to its subscribers.

SSL, EV SSL certificate and OSC subscribers are responsible for creation and protection of the access passwords belonging to their certificate keys.

6.4.2. Activation Data Protection

The authorized TURKTRUST personnel using the private keys belonging to root and sub-root certificates change access codes at least in 90 (ninety) days. Authorized people are responsible for protection and confidentiality of the access codes.

TURKTRUST subscribers are responsible for protection and confidentiality of the activation data belonging to their private keys in accordance with these recommendations indicated above.

6.4.3. Other Aspects of Activation Data

The delivery of TURKTRUST PINs is only valid for QEC owners. If this delivery is done via password envelope, a secure courier service will be contracted. The secure courier delivery is completed with the handwritten signature of the subscriber. The smart card that contains the QEC and the password envelope that contains the PIN are sent on two consecutive days. Hence, a measure is taken for not having both of them accessible at the same time by a third party.

In QEC activation method, the PIN is not transported in any electronic or physical way. The initial random PIN is kept in encrypted form in TURKTRUST database, and any user's access is turned off. In order to decrypt the code and access it from the database, the subscriber should connect the card to the PC and request activation through the TURKTRUST smart card management software. Even in this case, the subscriber's PC and TURKTRUST server communicate in encrypted manner. Thus, security of the PIN of the card which is delivered to its owner is not less than any time during the life cycle of the card.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Under the certification business processes carried out by TURKTRUST, 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 viruses, malicious and unauthorized software.
- Computer systems are protected against network security hacking.
- Access rights to computer systems and authentication are ensured by passwords supplied to TURKTRUST's personnel.
- Access rights to computers have been limited to the roles assigned to authorized persons.
- In particular, all transactions peculiar to CA services such as certificate enrollment, generation, suspension, revocation are saved in the database. In order to prevent unauthorized access and unintended modification of the database, several physical and electronic measures are taken at different access levels of authentication. Logical consistency at the database level adds another measure of security to preclude modification of a revocation status which would otherwise be assumed to be irreversible.
- 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.

- TURKTRUST uses trustworthy systems and products that are protected against modifications. In this regard, recommendations of CWA 14167-1 standard are strictly followed under continuous auditing of Information and Communication Technologies Authority of Turkey.

6.5.2. Computer Security Rating

Not applicable.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

System development controls are applied for development facility security (through facility security clearance certifications), development environment security, development personnel security, configuration management security during product maintenance and software development methodology (through ISO/IEC 27001 and ISO 9001 certifications). Details about these aspects and change management are documented in Information Systems Acquisition, Development and Maintenance Procedure.

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 TURKTRUST.

TURKTRUST 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 sub-root certificates of TURKTRUST's issuing certification authorities are used in environments where network security is ensured. Such systems are protected physically and technically.

All other systems within TURKTRUST are also protected by appropriate network security methods. All network elements such as firewalls, switches 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 TURKTRUST communicate records relating to their certification operations to TURKTRUST over the Internet by secure network connection.

6.8. Time-Stamping

During the execution of certification services of TURKTRUST, electronic records for certain operations contain time information synchronized by the 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 CP document describes the profiles of certificates issued and CRLs generated, and the structure of OCSP service by TURKTRUST.

7.1. Certificate Profile

TURKTRUST certificate profiles are based on the documents "ISO/IEC 9594-8/ ITU-T Recommendation X.509: "Information Technology- Open Systems Interconnection- The Directory: Public –key and attribute certificate frameworks" and "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Besides, TURKTRUST QEC profile also follows the document "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" ("Qualified Electronic Certificate, CRL and OCSP Request/Response Message Profiles") which was published by the Information and Communication Technologies Authority of Turkey.

TURKTRUST certificates basically contain the following fields:

Field Name	Description
Serial Number	Unique number within issuer scope
Signature Algorithm	Object identifier (refer to Section 7.1.3)
Issuer	Refer to Section 7.1.4
Start of Validity	UTC time encoded in accordance with RFC 5280
End of Validity	UTC time encoded in accordance with RFC 5280
Subject	Refer to Section 7.1.4
Public Key	Key value encoded in accordance with RFC 5280
Signature	Signature value encoded in accordance with RFC 5280

"Certificate Policy" field in TURKTRUST QEC contains "Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır. (This certificate is a qualified electronic certificate according to the Electronic Signature Law no. 5070)" mandatory statement as required by the Law.

7.1.1. Version Numbers

Root and sub-root certificates and end user certificates issued by TURKTRUST support the X.509 v3 version pursuant to the "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" document.

7.1.2. Certificate Extensions

TURKTRUST supports all certificate extensions defined in accordance with the RFC 3280 - X.509 v3 standard. According to the certificate type, the extensions of authority key identifier, subject key identifier, key usage, certificate policies, basic constraints, subject alternative name, SCRL distribution points and extended key usage are arranged in a proper form.

QECs contain the qualified electronic certificate extensions defined under the "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile" and "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" ("Qualified Electronic Certificate, CRL, and OCSP Request/Response Message Profiles") documents.

7.1.3. Algorithm Object Identifiers

For signing all the certificates issued by TURKTRUST, one of the algorithms below is used:

Algorithm Name	OID
SHA-1 with RSA	1.2.840.113549.1.1.5
SHA-256 with RSA	1.2.840.113549.1.1.11
SHA-384 with RSA	1.2.840.113549.1.1.12
SHA-512 with RSA	1.2.840.113549.1.1.13

For SSL, EV SSL and OSC SHA-1 usage will be abandoned after it becomes certain that at least one of the other algorithms is supported in all contemporary electronic signature applications. For QEC, related algorithms will be used according to the requirements of the legislation.

7.1.4. TURKTRUST Name Forms

Certificates issued by TURKTRUST use X.500 distinguished names.

7.1.5. Name Constraints

No anonymity or pseudonyms shall be used in qualified electronic certificates issued by TURKTRUST. 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 TURKTRUST, the relevant certificate policy object identifier number (OID) indicated in Section 1.2 of this CP document is used by the certificate type.

7.1.7. Usage of Policy Constraints Extension

TURKTRUST's sub-root certificates may contain policy constraints extension as necessary.

7.1.8. Policy Qualifiers Syntax

In the "certificate policy" extension of certificates issued by TURKTRUST, 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 TURKTRUST basically contain TURKTRUST'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. CRLs generated by TURKTRUST are in accordance with the document "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" ("Qualified Electronic Certificate, CRL, and OCSP Request/Response Message Profiles – April 2007") which was published by the Information and Communication Technologies Authority of Turkey.

7.2.1. Version Number

CRLs generated by TURKTRUST support the X.509 v2 version under the "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" document.

7.2.2. CRL and CRL Entry Extensions

CRLs generated by TURKTRUST use extensions defined in RFC 5280.

7.3. OCSP Profile

TURKTRUST 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. The OCSP responses generated by TURKTRUST are in accordance with the document "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" ("Qualified Electronic Certificate, CRL, and OCSP Request/Response Message Profiles – April 2007") which was published by the Information and Communication Technologies Authority of Turkey.

7.3.1. Version Number

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

7.3.2. OCSP Extension

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TURKTRUST is audited by the Information and Communication Technologies Authority under the e-signature legislation. Along with this audit, TURKTRUST SSL EV SSL and OSC processes are audited according to the ETSI TS 102 042 standard by an authorized auditing body.

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 conditions related to operations are kept under control via an internal audit plan.

TURKTRUST carries out risk assessments according to the ISO/IEC 27001 Information Security Management System. Therefore, business risks are evaluated and the necessary security conditions and operational procedures are determined. The risk analysis is regularly reviewed and revised if necessary.

8.1. Frequency and Circumstances of Assessment

The Information and Communication Technologies 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.

SSL, EV SSL and OSC processes are audited yearly according to the ETSI TS 102 042 standard and the certification is renewed every three years.

Pursuant to the ISO/IEC 27001 Information Security Management System certificate, follow-up audits on a yearly basis and a recertification audit in every third year are conducted.

Internal audit of ECSP processes are conducted every three months in accordance with ETSI TS 102 042 and BR, whereas the ISO/IEC 27001 Information Security Management System and TS EN ISO 9001 Quality Management System processes are audited internally twice a year.

8.2. Identification and Qualifications of Assessor

The Information and Communication Technologies Authority is the regulating and auditing agency designated by the Law.

The ETSI TS 102 042 audit is performed by a qualified auditing body that meets the requirements below:

- Qualified in PKI technologies, information security tools and techniques, information technologies, security audits and third party reporting.
- Accredited by a similar organization to the European Cooperation for Accreditation with respect to its conformity with the ISO/IEC 17021.
- Accredited with respect to its conformity with the provision 3.4 of the CEN Workshop Agreement (CWA) 14172-2 standard.

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

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

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 QECs in Turkey.

The ETSI 102 042 audit is performed by an independent and authorized auditing body.

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

TURKTRUST's institutional audit is conducted by TURKTRUST'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 TURKTRUST's electronic certification services, technical infrastructures used in providing such services and the facilities where such services are provided.

The ETSI 102 042 audit covers all the processes of SSL, EV SSL and OSC services, the technical infrastructure used while giving these services and the premises where the services are performed.

The ISO/IEC 27001 Information Security Management System certification covers TURKTRUST'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 TURKTRUST's activities and operation are found out, sanctions and penalties are imposed as indicated in the legislation.

TURKTRUST identifies the corrective and preventive actions about the minor non-conformities detected during the ETSI TS 102 042 conformance audit of the SSL, EV SSL and OSC processes. If the deficiencies detected are of major extent, this may lead to revocation of the related certificate and authorization.

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 TURKTRUST until the next audit.

Deficiencies detected in the internal audits conducted by TURKTRUST 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 TURKTRUST if deemed necessary. Non-communication of any result from the Institution means there is no adverse assessment.

The audit results of SSL, EV SSL and OSC processes that are audited according to the ETSI TS 102 042 standard shall be communicated officially to TURKTRUST by the auditing body.

The ISO/IEC 27001 Information Security Management System audit results shall be communicated officially to TURKTRUST 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 CP document describes TURKTRUST'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 TURKTRUST are priced differently depending on type.

QECs are priced according to their validity periods and 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.

SSL and EV SSL certificates and OSCs are priced according to certificate type, term and characteristics. Furthermore, during pricing of SSL and EV SSL certificates, the extent of material transaction limits, the commercial general liability insurance and the professional liability insurance are also taken into account.

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

9.1.2. Certificate Access Fees

Certificates issued by TURKTRUST are kept accessible to the public provided that subscribers 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 TURKTRUST 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 QECs as required by the Law.

Access services on revocation or status information provided by TURKTRUST for SSL and EV SSL certificates and OSCs are also free of charge.

9.1.4. Fees for Other Services

TURKTRUST 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

TURKTRUST does not refund for QECs, SSL and EV SSL certificates and OSCs. However, if the certificate contains information different than that on the application due to causes attributable to TURKTRUST, a new certificate shall be issued free of charge, or it is refunded upon request.

9.2. Financial Responsibility

TURKTRUST 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.

TURKTRUST is under obligation to carry commercial general liability insurance and professional liability insurance in accordance with the ETSI TS 102 042 standard concerning SSL and EV SSL services.

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.

In addition to the certificate financial liability insurance done for the QECs, SSL and EV SSL certificates are covered by commercial general liability insurance and professional liability insurance indicated below.

The commercial general liability insurance covers all direct and indirect damages that can be linked to the SSL and EV SSL services. Professional liability insurance covers the legal responsibilities arising from damages that may be caused by the professional activities of TURKTRUST about the SSL and EV SSL services.

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End-Users

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

In addition, TURKTRUST is under obligation to carry commercial general liability insurance and professional liability insurance in accordance with the ETSI TS 102 042 standard concerning SSL and EV SSL services.

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 TURKTRUST's certification services, private keys of root and sub-root certificates of TURKTRUST'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 TURKTRUST 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 TURKTRUST 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 TURKTRUST's internal audit.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

TURKTRUST, 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 TURKTRUST shall be used for certification services, and customer 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 TURKTRUST'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 TURKTRUST 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

TURKTRUST may use the certificate, seal, and information contained therein provided in the certificate application for the purposes set out in this CP and CPS and subscriber's agreement or letter of commitment

9.4.6. Disclosure Pursuant to Judicial and Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

Not applicable.

9.5. Intellectual Property Rights

TURKTRUST holds the intellectual property rights on all certificates issued by TURKTRUST, 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 TURKTRUST 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.

As regards to SSL and EV SSL certificates, TURKTRUST specifically warrants that:

- Legal Existence: TURKTRUST has confirmed that, as of the date the SSL and EV SSL certificate was issued, the Subject named in the SSL and EV SSL certificate legally exists as a valid organization or entity;
- Identity: TURKTRUST has confirmed that, as of the date the SSL and EV SSL certificate was issued, the legal name of the Subject named in the SSL and EV SSL certificate matches the name on the official government records;
- Right to Use Domain Name: TURKTRUST has taken all steps reasonably necessary to verify that, as of the date the SSL and EV SSL certificate was issued, the Subject named in the SSL and EV SSL certificate has the exclusive right to use all the Domain Name(s) listed in the EV SSL certificate;
- Authorization for SSL and EV SSL Certificate: TURKTRUST has taken all steps reasonably necessary to verify that the Subject named in the SSL and EV SSL certificate has authorized the issuance of the EV SSL certificate;
- Accuracy of Information: TURKTRUST has taken all steps reasonably necessary to verify that all of the other information in the SSL and EV SSL certificate is accurate, as of the date the SSL and EV SSL certificate was issued;
- No Misleading Information: While the issuance of the SSL and EV SSL certificate, TURKTRUST implements a procedure that is mentioned in CPS, for reducing the likelihood that the information contained in the certificate's subject fields that would be misleading;
- Letter of Commitment: The Subject named in SSL and the EV SSL certificate has entered into a legally valid and enforceable Letter of Commitment with TURKTRUST that satisfies the requirements of this CPS or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
- Status: TURKTRUST follows the requirements of this CPS and maintain a 24 x 7 online-accessible repository with current information regarding the status of the SSL and EV SSL certificate as valid or revoked; and
- Revocation: TURKTRUST follows the requirements of this CPS and revoke the SSL and EV SSL certificate for any of the revocation reasons specified in the CA/Browser Forum Guidelines.

In particular to EV SSL certificate beneficiaries listed below, warranties mentioned in this section do apply:

- The Subscriber entering into the Subscriber Agreement for the EV SSL certificate;
- The Subject named in the EV SSL certificate;

- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its certificate in software distributed by such Application Software Suppliers;
- All Relying Parties that actually rely on such EV SSL certificate during the period when it is Valid.

Issuing certification authorities under TURKTRUST fulfill CA obligations stated in Article 10 of the Law and Article 14 of the Regulation to issue QECs, and the ETSI TS 102 042 and BR obligations to perform SSL, EV SSL and OSC services.

9.6.2. Registration authority Representations and Warranties

Registration centers under TURKTRUST represent and warrant that identity validation have been performed accurately and reliably for the applicants according to the certificate types as stated in this CPS document, 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 TURKTRUST 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 or the letter of commitment.

Subscribers of QECs have to fulfill obligations stated in Article 15 of the Regulation along with the stipulations in the subscriber's agreement or the letter of commitment.

9.6.4. Relying Party Representations and Warranties

Subscribers and relying people are under obligation to check the validity of electronic signature generated based on TURKTRUST's QECs.

The owners of SSL and EV SSL certificates and OSCs and the relying parties are under obligation to check the validity of the contents of the certificates issued by TURKTRUST when they rely on them.

9.6.5. Representations and Warranties of Other Participants

Other participants which are comprised of all persons and organizations which TURKTRUST cooperates with and from which TURKTRUST procures services during certification services represent and warrant that they provide the services reliably and accurately and not disclose confidential or private information regarding TURKTRUST's processes and customers. TURKTRUST 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 TURKTRUST 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.

Mandatory certificate financial liability insurance for QECs covers 10.000 TL per occurrence and 1.000.000 TL in the aggregate for the yearly policy term.

Certificate financial liability insurance for SSLs covers 10.000 TL per occurrence and 1.000.000 TL in the aggregate for the yearly policy term.

For SSL and EV SSL certificates, commercial general liability insurance covers USD 2.000.000 per occurrence and in the aggregate for the yearly policy term and professional liability insurance covers USD 5.000.000 per occurrence and in the aggregate for the yearly policy term.

9.9. Indemnities

If TURKTRUST 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, TURKTRUST shall indemnify any such damage.

Pursuant to Article 13 of the Law, TURKTRUST 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 TURKTRUST proves its faultlessness, then it is relieved of such obligation of indemnification.

Where subscribers fail to fulfill their obligations under the subscriber's agreement or letter of commitment and TURKTRUST or third parties suffer damages due to such failure, the subscriber shall indemnify such damage.

9.10. Term and Termination of CP Documentation

9.10.1. Term

This version of the CP 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 CS document depending on changes and arrangements that may occur in TURKTRUST'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 TURKTRUST.

9.10.3. Effect of Termination and Survival

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

Where it becomes necessary to make changes in certificates issued by TURKTRUST 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 TURKTRUST.

9.11. Individual Notices and Communications to Participants

Available contact information of subscribers are used for all individual notices from TURKTRUST to subscribers.

Notices from TURKTRUST 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 CP document depending on changes and arrangements that may occur in TURKTRUST's activities and certification services, a new CP document version which covers relevant changes shall be prepared and published by TURKTRUST upon the approval of the board of management of TURKTRUST.

While the CP 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. TURKTRUST 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 CP document depending on changes and arrangements that may occur in TURKTRUST's activities and certification services, a new CP document version which covers relevant changes shall be prepared and published by TURKTRUST.

The related principles and practices set forth in the CP CPS document are reviewed annually during management review meetings.

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 TURKTRUST 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 TURKTRUST's activities and certification services and amendments to the present CP and CPS documents occur, subscribers and relying parties 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, TURKTRUST shall use all reasonable means to notify subscribers and relying people.

The new CP and CPS versions shall be published in the TURKTRUST 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 TURKTRUST and subscribers and relying parties, 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 Ordinances and Communiqués issued by the Information and Communication Technologies Authority. The Institution is responsible for regulating and auditing the CA's operations under the Law.

9.15. Compliance with Applicable Law

TURKTRUST provides QEC services in accordance with the "Electronic Signature Law" no.5070 and the Ordinances and Communiqués issued by the Information and Communication Technologies 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 TURKTRUST which reflect the changes.

9.16.4. Waiver of Rights

Not applicable.

9.16.5. Force Majeure

Any circumstance which obstructs TURKTRUST's performance of activities relating to electronic certification service provision and is normally beyond TURKTRUST's control is called a force majeur. While such forces majeurs continue to be effective, TURKTRUST'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.