CERTIFICATION PRACTICE STATEMENT

(CPS)

(For DV SSL, OV SSL, OSC and similar electronic certificates)

VERSION : 11

DATE : 21.11.2016

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 Regulation and the Communiqué issued pursuant to the Law by the Information and Communications Technologies Authority of Turkey and international standards.

This documentation named the Certificate Practices Statement (CPS) has been prepared by TURKTRUST, in order to disclose how TURKTRUST performs its operations of electronic certificate services excluding qualified electronic certificates provision, in conformity to the "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

Regarding SSL (Secure Socket Layer) 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 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. In the event of any inconsistency between this CPS document and those ETSI TS 102 042 and Baseline Requirements document, the requirements in those documents take precedence over this CPS document. Compliance to those documents includes "Publicly-Trusted Certificate Policy - Baseline Requirements (PTC-BR)" found in the ETSI TS 102 042 standard.

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

1.1. Overview

This CPS document covers electronic certificate services except qualified electronic certificates services provided by TURKTRUST. The practice principles included in CPS cover all of TURKTRUST's practices of customer services, registration authorities and issuing certification authorities.

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

The electronic certificate services of TURKTRUST are executed via procedures, instructions and customer guides that are prepared based on practice principles that exist in the CPS document which are documented in accordance with ETSI TS 102 042 Electronic Signatures Infrastructure (ESI); Policy Requirements for Certification Authorities Issuing Public Key Certificates standard, ISO/IEC 27001 Information Security Management System together with ISO 9001 Quality Management System.

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. Due to this evaluation or any requirements arising throughout the year, those documents are revised if necessary.

1.2. Document Name and Identification

This CPS document is named as the "TURKTRUST Certification Practice Statement (CPS) (For DV SSL, OV SSL, OSC and similar electronic certificates)". The version number and date of the document is provided herein on the cover page.

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

- TURKTRUST OV SSL Certificate Policy (2.16.792.3.0.3.1.1.2) covers OV SSL certificates for servers. OV 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 DV SSL Certificate Policy (2.16.792.3.0.3.1.1.6) covers DV SSL certificates for servers. DV SSL Certificates are issued and maintained in conformity with "Normalized Certificate Policy" defined in ETSI TS 102 042.

This CPS 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 practice statement are CA units offering certification services, customers receiving the service and users.

1.3.1. Issuing Certification Authorities

Issuing certification authorities are the units of CAs responsible for issuing, 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.

1.3.2. Registration Authorities

Registration authority is CA unit that offers services to end users directly such as certificate application, renewal and revocation. This unit establish customer records; perform identification and authentication processes and direct relevant certificate requests to issuing certification authorities.

Actions associated with registration center are performed by registration unit within the TURKTRUST center in response to certificate requests arriving from TURKTRUST sales representatives. 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. Consequences due to the use of a certificate and liability of the subscriber are qualified by the relevant legislation and subscriber's letter of commitment.

1.3.4. Relying Parties

Relying parties are those who receive documents signed by the private keys based on the electronic 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 electronic 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 electronic 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.

Server certificates (DV orOV SSL) 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

Use of TURKTRUST electronic certificates beyond the control of the subscriber is disallowed. TURKTRUST certificates cannot be used outside the limits and scope declared in this 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 to which this CPS document is subordinate.

1.5.1. Organization Administering the CPS Document

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

1.5.2. Contact Person

Contact information for this CPS 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 : 0 850 222 444 6
E-mail : sertifika@turktrust.com.tr
Web : http://www.turktrust.com.tr

1.5.3. Person Determining CPS Suitability for the Policy

TURKTRUST's senior management determines the suitability of this CPS document with the CP document.

1.5.4. CPS Approval Procedure

This CPS document of TURKTRUST has been prepared in compliance with the TURKTRUST CP document. CPS document is approved by the board of management of TURKTRUST. CPS so approved shall be used to regulate and run the CA activities.

The senior management of TURKTRUST is responsible for ensuring that the certification practices established to meet the applicable requirements specified in this CPS are properly implemented.

Regarding OV SSL (Secure Socket Layer) 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 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. In the event of any inconsistency between this CPS document and those ETSI TS 102 042 and Baseline Requirements document, the requirements in those documents take precedence over this CPS document.

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

DV : Domain Validation

ETSI : European Telecommunication Standards Institute

IETF : Internet Engineering Task Force

OCSP : On-line Certificate Status Protocol

OID : Object Identifier

OSC : Object Signing Certificate

OV : Organization Validation

PKI : Public Key Infrastructure

PTC-BR: Publicly-Trusted Certificate - Baseline Requirements

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

SAN : Subject Alternative Name

SSL : Secure Sockets Layer

TCKN : Republic of Turkey the Number of Citizenship.

TSE : Turkish Standards Institution

1.6.2. Definitions

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.

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.

DV SSL Certificate: The SSL certificate issued and maintained in accordance with the "Domain Validation Certificate Policy" defined in ETSI TS 102 042 standard.

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.

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

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.

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.

OV SSL Certificate: The SSL certificate issued and maintained in accordance with the "Organization Validation Certificate Policy" defined in ETSI TS 102 042 standard.

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.

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.

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.

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.

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.

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 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.

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 datedness 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. Within the scope of electronic certificates, 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.

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. Only exception to the validity period of CRL is the expiry date of root or sub-root certificates. Expiry date of a root or a sub-root certificate is written to the NextUpdate field of the CRL if the next update of the CRL exceeds the validity period of a root or a sub-root certificate.

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 electronic certificate applicants or renewal requestors 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.

Server names authenticated by TURKTRUST are used in the server certificates. The names of legal entities or real persons, which in any case are validated according to legal documents, are used in object signing certificates Name fields of root and sub-root certificates include explicitly the commercial title and relevant root information of TURKTRUST.

3.1.3. Anonymity or Pseudonymity of Subscribers

TURKTRUST does not issue electronic certificates that include anonymity or pseudonymity.

3.1.4. Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

Electronic certificates issued by TURKTRUST allow unique identification of subscribers with information contained in DN. Relevant data providing uniqueness in DN is explained in this section.

3.1.5.1. DV SSL and OV (Commercial Entities Resident in Turkey)

In order to distinguish the subscriber uniquely, DN in TURKTRUST server certificates are conditioned.

For TURKTRUST DV SSL certificates only domain name verification is executed and no kind of organizational verification is executed. Because of the verification level of DV SSL certificates, only domain name is included in the certificate content and no kind of information regarding the legal entity is included in the certificate content.

DN field for incorporations resident in Turkey:

- "CN" contains server name registered in DNS under the name of the subscriber
  - In wildcard DV SSL and OV SSL certificates, CN field contains "*.<DNS name>". This field cannot contain "*.com" or "*.com.tr" which do not show the fully qualified domain name.
  - CN field cannot contain IP addresses or internal server names in DV SSL or OV SSL certificates.
- "O" contains the complete name of incorporation as in Turkish Trade Register or any abbreviations used are locally accepted.

- "OU" contains the organizational unit or a trademark which is registered in Turkish Standards Institution.
- "L" contains city of incorporation which is indicated in Turkish Trade Register.
- "C" contains country code of incorporation that is listed in ISO 3166-1 standard.
- "SAN" contains the "DNS" which is indicated in "CN" field. Provided that domain name ownership or the authority to control the domain name for server certificates is verified for each domain name, more than one domain name can be written in this field. The constraints which are specified in "CN" are also valid for SAN field.

DN field for public entities in Turkey:

- "CN" contains server name registered in DNS under the name of the subscriber.
    - For DV SSL and OV SSL wildcard certificates in CN field "*.<DNS name>" is written. This field cannot contain "*.com" or "*.com.tr" which do not show the fully qualified domain name.
    - CN field cannot contain IP addresses or internal server names in DV SSL or OV SSL certificates.
- "O" contains the complete name of the public entity as in applicable Turkish legislation, possibly in the law of establishment or in any other legislation or any abbreviations used is locally accepted.
- "OU" contains the organizational unit or a trademark which is registered in Turkish Standards Institution.
- "L" contains city of public entity which is indicated in Turkish Trade Register.
- "C" contains country code of public entity that is listed in ISO 3166-1 standard.
- "SAN" contains the "DNS" which is indicated in "CN" field. Provided that domain name ownership or the authority to control the domain name for server certificates is verified for each domain name, more than one domain name can be written in this field. The constraints which are specified in "CN" are also valid for SAN field.

DN field for non-commercial entities (associations, foundations, chambers or unions) in Turkey:

- "CN" contains server name registered in DNS under the name of the subscriber.
    - For DV SSL and OV SSL wildcard certificates in CN field "*.<DNS name>" is written. This field cannot contain "*.com" or "*.com.tr" which do not show the fully qualified domain name.
    - CN field cannot contain IP addresses or internal server names in DV SSL or OV SSL certificates.
- "O" contains the complete name of non-commercial entities as in applicable official records or any abbreviations used are locally accepted.
- "OU" contains the organizational unit or a trademark which is registered in Turkish Standards Institution.
- "L" contains city of non-commercial entities which is indicated in Turkish Trade Register.
- "C" contains country code of non-commercial entities that is listed in ISO 3166-1 standard.

- "SAN" contains the "DNS" which is indicated in "CN" field. Provided that domain name ownership or the authority to control the domain name for server certificates is verified for each domain name, more than one domain name can be written in this field. The constraints which are specified in "CN" are also valid for SAN field.

DN field for other business entities (ordinary partnership or real persons) in Turkey:

- "CN" contains server name registered in DNS under the name of the subscriber.
  - For DV SSL, OV SSL wildcard certificates in CN field "*.<DNS name>" is written. This field cannot contain "*.com" or "*.com.tr" which do not show the fully qualified domain name.
  - CN field cannot contain IP address or internal server names in DV SSL or OV SSL certificates.
- "O" contains the complete name of business entity as in applicable official records such as a recent document showing the accrued tax or any abbreviations used are locally accepted.
- "OU" contains the organizational unit or a trademark which is registered in Turkish Standards Institution.
- "L" contains city of other business entities which is indicated in Turkish Trade Register.
- "C" contains country code of other business entities that is listed in ISO 3166-1 standard.
- "SAN" contains the "DNS" which is indicated in "CN" field. Provided that domain name ownership or the authority to control the domain name for server certificates is verified for each domain name, more than one domain name can be written in this field. The constraints which are specified in "CN" are also valid for SAN field.

3.1.5.2. DV SSL and OV SSL (Commercial Entities Not Resident in Turkey)

DN in server 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.

3.1.5.3. OSC

DN in TURKTRUST OSC is formed as below:

- "CN" contains complete name of the subscriber, which is based on the official documentation according to the legislation of residence.

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.

TÜRKTRUST verifies the trademark stated in the OV SSL certificate application forms. In the case the domain name includes country code (".tr") TURKTRUST will confirm trademark via nic.tr verification. Additional tradename verification will not be required. If and when domain name does not include a country code, TURKTRUST verify trademark according to related country's regulation and legislation.

TURKTRUST will require a Tradename Registry Letter for national OV SSL and OSC applications which do not include a country code in the domain name. Also for international applications an equivalent document of Trademark Registry Letter is required.

Notwithstanding this clause, TURKTRUST holds right to deny an application 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

Certificate applicants prove their possession of the private key by submitting a PKCS#10 or equivalent file to TURKTRUST. 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 shall be verified against the official documents of the country of residence of the applicant. Verification herein is executed according to the TURKTRUST procedures.

3.2.2.1. DV SSL, OV SSL or OSC

For DV SSL certificates legal entity verification is not executed.

For OV SSL and 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 OV SSL and OSC applications, different control steps are applied depending on whether the request is domestic or foreign. The residential address of the subscriber is based on while determining of such distinction. Subscribers' legal existence and credentials, domain name, applicant's representative's and application's existence, CSR information and so forth informations should be verified This verification is done with a unique user name and activation code sent to the authorized person's e-mail address.

3.2.3. Non-verified Subscriber Information

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

3.2.4. Validation of Authority

For OV SSL applications and in such case if the subscriber is a legal entity for an OSC application, the existence of the applicant's representative and the existence of the application are verified via an independent information source as specified in TURKTRUST procedures.

3.2.5. 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

For server certificates and OSCs renewal and rekey is not performed.

3.3.2. Identification and Authentication for Re-key after Revocation

For server certificates and OSCs rekey is not performed and certificate application procedures are applied like a first time application.

3.4. Identification and Authentication for Revocation Request

TURKTRUST receives revocation requests for server certificates and OSCs 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 or applicant's representative connects to interactive certificate operations in the 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 practices set forth in this CPS. In what follows, different practices 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 OSC.

For server certificates and OSCs, 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.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Server certificate 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.

- For an OV SSL or OSC application, if the subscriber is a legal entity, business entity or a private organization, not having a trade registry record. If the subscriber is a government entity, not having a governmental record.
- In 30 (thirty days) after the enrollment of an OV SSL or OSC application, CSR is not delivered to TURKTRUST.
- For a server certificate or OSC application, there emerges a strong opinion that issuing the certificate may damage TURKTRUST reputation.
- For a server certificate application, except for the applications from governmental entities, payment is not made.

During server certificate applications "Certification Authority Authorization (CAA)" records identified in CA/Browser Forum's BR document, are not controlled by TURKTRUST and no kind of action is performed in accordance with these records.

4.2.3. Time to Process Certificate Applications

Server certificate 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.

Certificate is issued within at most 1 (one) working day once a certificate application is accepted with regard to the principles stated in Section 4.2.2.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

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

OV SSL certificates and OSCs are created by two authorized persons in trusted roles, who are responsible for production, connecting to the system and giving approval for production.

4.3.2. Notification to Subscriber of Issuance of Certificate

After electronic 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 the electronic all certificate types before installing or using the electronic 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.

TURKTRUST generates two test certificates for all sub-root certificates that sign generated DV SSL and OV SSL certificates allowing third parties to test their certificates and published these certificates via a test web page with revoking one of the test certificates.

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 dependent on standards, other regulatory actions and stipulations indicated in the CP and CPS documents and the related subscriber's 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 letters of commitment.

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 dependent on standards, 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 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

For server certificates and OSCs, certificate renewal is not performed and certificate application procedures are applied like a first time application. As the result of this application a new certificate with a new key pair is generated.

4.7. Certificate Re-key

For server certificates and OSCs, certificate renewal is not performed and certificate application procedures are applied like a first time application. As the result of this application a new certificate with a new key pair is generated.

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 principles stated in Section 4.1.

4.8.2. Who May Request Certificate Modification

Principles of Section 4.1.1 apply.

4.8.3. Processing Certificate Modification Requests

Principles of Section 3.2 apply.

4.8.4. Notification of New Certificate Issuance to Subscriber

Principles of Section 4.3.2 apply.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Principles of Section 4.4.1 apply.

4.8.6. Publication of the Modified Certificate by the CA

Principles 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 server certificates and OSCs revocation process is completed within 24 (twenty four) hours. Suspension process is not applied for server certificates 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.
- 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 OV SSL certificates,
- If an evidence is obtained 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 server 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 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 server certificates,
- 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 of TURKTRUST for server 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,

4.9.1.2. TURKTRUST's Sub-root Certificates

Where a sub-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'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 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 server 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 OSCs,
- System registered server administrator of the legal entity or the persons authorized to represent the legal entity subscriber for DV SSL certificates,
- The legal entity authorized to represent the legal person subscriber for OV SSL certificates and OSCs,
- 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 server certificates 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. Upon the verification of revocation request letter, the revocation action is completed. The revocation status after the action is notified by e-mail to the authorized personnel or applicant's representative.

If and when subscriber prefers to revoke the certificate via web site, the server administrator or applicant's representative 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 or applicant's representative.

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 site 7 days and 24 hours, following the approval of the request and authentication of identity. Revocation requests transmitted on paper are taken into evaluation immediately during working hours and necessary actions are carried out within at most 24 (twenty four) hours.

4.9.6. Revocation Checking Requirements for Relying Parties

Relying parties are under obligation to verify the relevant certificate before relying on an electronic certificate transmitted. To verify a certificate's status, updated CRLs published by TURKTRUST or OCSP, the on-line certificate status inquiry service, should be used.

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, revoked, 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 by e-mail.

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

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

For root or sub-root certificates of TURKTRUST suspension is not performed.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Certificate Suspension

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

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 (twenty four) hours even if there is no change in the status of certificates.

Only exception to the validity period of CRL is the expiry date of root or sub-root certificates. Expiry date of a root or a sub-root certificate is written to the NextUpdate field of the CRL if the next update of the CRL exceeds the validity period of a root or a sub-root certificate.

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 (good, revoked or 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 uses backup systems to prevent interruption of OCSP service.

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 CPS 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 center is constantly controlled.

The perimeter of the facility has been surrounded by protection to prevent uncontrolled access or exit. Security personnel man all entry-exit points to the center. Physical access to secure areas is allowed via the pass card entry control system. Unauthorized persons are prohibited to enter certain areas. High-security areas where basic certificate generation is carried out are always closed to unauthorized access. Entries and exits are logged. As an additional security measure, critical areas and passes are monitored by cameras and daily recording of cameras is kept for security reasons. Furthermore, visitors who are present in the building for maintenance and support activities, meetings and similar reasons are not left alone and oversighted by an authorized TURKTRUST personnel.

5.1.3. Power and Air Conditioning

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

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

5.1.4. Water Exposures

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

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

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

5.1.5. Fire Prevention and Protection

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

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

5.1.6. Media Storage

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

5.1.7. Waste Disposal

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

All other waste of the building and 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 Responsibles:** Employees responsible for routine certification services such as customer services, document control, processes relating to certificate registration, generation, suspension for QEC 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.

Appointment of the personnel who will be assigned to trusted roles is done by TURKTRUST senior management according to the related procedures.

Senior management, executive managers and all personnel in trusted roles, are not engaged in any commercial or financial activies and conflicting interests that might prejudice the impartiality of trust in the services TURKTRUST provides.

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, disposal 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.

Specifically, a user that is authorized to assume a Security Officer or Registration and Customer Services Officer role is not authorized to assume a System Auditor role. A user that is authorized to assume a System Administrator role is not authorized to assume a Security Officer or a System Auditor role.

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

5.3.5. Job Rotation Frequency and Sequence

TURKTRUST's security personnel and operators shall be subjected to rotation in sub-duties within their field of work. Unless there is a permanent change of assignment, no routine rotations shall be made between different 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.

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. Exact time of logs are taken from the related servers that are synchronized by the time source used for time-stamping services.

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 during active life cycle in the system. 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. Generation of audit logs is invoked at software start-up and cease only at software shutdown.

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 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 regarding server certificates and OSCs shall 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.

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

5.5.4. Archive Backup Procedures

Backups of electronic archives are retained pursuant to 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 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.

Where the expiry of a root certificate draws closer, the term of an end user certificate to be issued shall be designated not to go beyond the expiry of any of the associated root certificates.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Where incidents or security compromises occur which would prevent TURKTRUST's operations, intervention is made pursuant to TURKTRUST's incident management procedure

and business continuity management procedure and business continuity plans. Incidents that were recognized and reported by TURKTRUST personnel and intervention to security breaches and troubleshooting methods are clearly mentioned in aforementioned documents.

There exists a Certificate Security Problem Notification Form on TURKTRUST web site for TURKTRUST subscribers or third parties to notify security troubles encountered during their certificates' usage. The security breach notification submitted here is evaluated by TURKTRUST and if deemed necessary, TURKTRUST return is made within the shortest period of time.

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. In particular, real time web services such as OCSP and CRL can be made available in a maximum period of 2 hours through DRC once a need arises. Similarly, other certificate services such as enrollment, suspension, revocation etc. can be evoked at DRC to serve without loss of data or business interruption on a 24x7 hours basis. As regards to controls ensuring robustness of this policy, periodic practices are conducted according to the related 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.

Furthermore capacity planning is done annually by the technical personnel and presented to the senior management. As part of this capacity planning changed demands in CA activities are fulfilled without service interruption. On the other hand these capacity demands are monitored by the senior management and related department managers. Projections of future capacity requirements in budget activities and financial management are made to ensure that adequate processing power and storage are available.

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 through public notice and direct e-mails to subscribers. In such case, TURKTRUST generates the last CRL log and destroys its own private key and backups.

Server certificate and OSC subscribers become aware of the termination of the activities via above public announcement and e-mails. 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 CPS 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, dissemination and disposal for root certificates under the dual control of authorized personnel as described in Section 5.1.2 in a technically and administratively secured environment.

During the generation of TURKTRUST DV SSL and OV SSL root and sub-root certificate key pairs the requirements of ETSI TS 102 042 and Baseline Requirements documents are fulfilled. As mentioned in these requirements a qualified auditor witnesses the generation of root certificate key pairs and/or the video of the entire process is recorded.

Private keys are protected against unauthorized access by physical and technical security measures. Dual control for this process is achieved by password controls and biometric checks. The system is evoked only if each of the two authorized persons logs into the system successively by entering password credentials and biometric data.

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.

Server administrators or applicant's representatives 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 applicants who will apply for server certificates or object signing certificates are responsible for a secure key generation during application.

By using the information received and verified during server certificate and OSC application, the subscriber is informed via e-mail about the certificate generation. Via domain that is used by the subscriber to send the CSR file during the application, certificate upload is ensured.

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 published at http://www.turktrust.com.tr accessible by relying people. The thumbprint information that belongs to root certificates shall be published in three (3) most circulated newspapers in Turkey. Thus, relying people may use public keys of TURKTRUST.

6.1.5. Key Sizes

TURKTRUST's root and sub-root certificates are 2048 bit length when and if RSA keys are used. And also for all end user certificates, 2048 bit RSA key pairs are used.

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

6.1.6. Key Generation and Quality Checking

Root and sub-root certificate key pairs are generated in hardware security modules that have appropriate security levels in accordance with the parameters specified in standards or regulations.

For DV SSL, OV SSL and OSC end user certificates, where key generation takes place on the customer side, the customer is responsible for generating the private key in appropriate tools and in appropriate 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. Furthermore given and system registered certificate content data is checked against the data in the CSR sent by the subscriber and in case of any inconsistency the CSR is denied.

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 international standards. 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.

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.

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, dissemination and disposal procedure.

The private keys of root and sub-root certificates of TURKTRUST are backed up in secure tokens that are EAL4+ or FIPS 140-2 Level 3 certified. These tokens are stored off-site in secured vaults. In need of a key recovery, these tokens can be used with appropriate credentials and by authorized persons to reload the private keys into the relevant HSMs. These backup and recovery operations for private keys are conducted under the dual control of authorized personnel as described in Section 5.2.2 in a technically and administratively secured environment.

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 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.

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 server certificates 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 server certificates 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 key deletion function of related HSM sand the operations performed are logged according to procedures. For this operation, at least two persons should be present.

There is no stipulation for destroying private keys of end user server certificates and OSCs upon certificate revocation or expiry. However, it is advised that the subscriber to destroy his private key.

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.

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 DV SSL and OV 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 electronic certificates cannot exceed 3 years.

The term for root and sub-root certificates of TURKTRUST's issuing certification authorities for server certificates and OSCs cannot exceed 30 (thirty) 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 passphrase 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.

Server 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

Not applicable.

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 the Information and Communications 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 Design Control Procedure and 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. According to the related procedures, such network elements are constantly monitored, internal or external attacks and unauthorized access attempts are detected and by means of other

security controls intrusions are blocked. Furthermore it is ensured to resolve the found vulnerabilities and breaches as a result of the systematic vulnerability and penetration tests.

Any kind of external access to TURKTRUST network is ensured via encrypted channels and only access to the provided services is allowed. Access to the systems which have sensitive data can be performed only via authorized networks that are present in TURKTRUST center.

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

TURKTRUST performs its operations regarding network security according to Communication and Operation Management Procedure, meeting the requirements of ETSI TS 102 042, Baseline Requirements and Network and Certificate System Security documents. These requirements can be listed generally as seen below;

- TURKTRUST effectively regulates the administration of user account management, auditing and modification or removal of access rights of the personnel who has direct access to the CA system.
- In case of privilege change for a personnel in trusted role who has direct access to the system (e.g. System and Network Administrator), passwords belonging to all accounts within the scope of authority of this personnel are changed.
- All user accounts are checked periodically and inoperative accounts are closed.
- Upon termination of a personnel's employment, all accounts of this personnel on the system are closed.
- System and Network Administrator decides after considering whether the patches or updates for network security software components are applied, postponed or not applied at all.
- For CA systems a user account is locked after defined value of wrong password entries.
- System logs are periodically reviewed by the system auditor and reported immediately to the management if any problem is detected.
- CA systems are subjected to vulnerability tests at latest once per 3 (three) months and penetration tests at least once a year. Results of these tests are evaluated and arrangements on the system are made.

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 CPS 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".

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

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

DV SSL certificates issued by TURKTRUST contain the following extensions:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer TURKTRUST certificate.
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Signing, key encipherment, data encipherment, and key agreement fields are set.
Certificate Policies	No	• Policy Identifier OID: 2.16.792.3.0.3.1.1.6 • Policy Qualifier Info – CPS: http://www.turktrust.com.tr/sue
Basic Constraints	No	CA marked “false”.
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the TURKTRUST OCSP service.
Extended Key Usage	No	Server authentication and client authentication values are set.

OV SSL certificates issued by TURKTRUST contain the following extensions:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer TURKTRUST certificate.
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Signing, key encipherment, data encipherment, and key agreement fields are set.
Certificate Policies	No	• Policy Identifier OID: 2.16.792.3.0.3.1.1.2 • Policy Qualifier Info – CPS: http://www.turktrust.com.tr/sue
Basic Constraints	No	CA marked “false”.
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the TURKTRUST OCSP service.
Extended Key Usage	No	Server authentication and client authentication values are set.

OSCs issued by TURKTRUST contain the following extensions:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer TURKTRUST certificate.
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Signing and non-repudiation fields are set.
Certificate Policies	No	• Policy Identifier OID: 2.16.792.3.0.3.1.1.4 • Policy Qualifier Info – CPS: http://www.turktrust.com.tr/sue
Basic Constraints	No	CA marked “false”.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the TURKTRUST OCSP service.
Extended Key Usage	No	Code signing and commercial software publishing values are set.

Server certificates and OSCs issued by TURKTRUST contain the following OCSP extensions:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer TURKTRUST certificate.
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	No	Signing, field is set.
Basic Constraints	No	CA marked “false”.
Extended Key Usage	No	OCSP signing values are set.
OCSP No Check	No	The extension which indicates that self-validity check for the OCSP certificate is not needed.

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

In all server certificate and OSC subscriber certificates SHA-256 algorithm is used. Root certificates which are for generating subscriber certificates still have SHA-1 or SHA-256 algorithm. But in all newly generated root and sub-root certificates SHA-256 algorithm is used, there is no new root and sub-root certificate generation with SHA-1.

7.1.4. TURKTRUST Name Forms

Certificates issued by TURKTRUST use X.500 distinguished names.

The full name of TURKTRUST is written in "O" (organization) fields as "TURKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.".

DV SSL certificates issued by TURKTRUST contain the following "Subject" fields:

"CN"	Values explained in Sections 3.1.5.2 and 3.1.5.3 of this document.
"OU"	"Domain Validated (DV) – WindSSL (R)"

OV SSL certificates issued by TURKTRUST contain the following "Subject" fields:

"CN"	Values explained in Sections 3.1.5.2 and 3.1.5.3 of this document.
"C"	Country code of the subject.
"S"	Optional. State or province of the subject.
"L"	Subject's city of residence.
"O"	Values explained in Sections 3.1.5.2 and 3.1.5.3 of this document.
"OU"	Optional. Organizational unit of the subject.

OSCs issued by TURKTRUST contain the following "Subject" fields:

"CN"	The exact full name of the subject, which is certifiable in accordance with the legislation in the country of the subject.
"C"	"TR"
"S"	Optional. State or province of the subject.
"L"	Subject's city of residence.
"O"	Optional. The exact full name of the subject organization, which is certifiable in accordance with the legislation in the country of the subject.
"OU"	Optional. Organizational unit of the subject.

7.1.5. Name Constraints

No anonymity or pseudonyms shall be used in certificates issued by TURKTRUST.

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 CPS document is used.

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.

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.

7.3.1. Version Number

The OCSP service provided by TURKTRUST supports the v1 protocol version under the "IETF RFC 6960 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 6960 may be used when necessary. However, it is not mandatory to use all extensions other than the basic OCSP information.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TURKTRUST OV SSL 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 and TS EN ISO 9001 Quality Management System certificates.

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 ETSI TS 102 042 standard and 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

OV SSL 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 and TS EN ISO 9001 Quality Management System certificates, 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 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 and TS EN ISO 9001 Quality Management System certifications shall be conducted by 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 ETSI 102 042 audit is performed by an independent and authorized auditing body.

The ISO/IEC 27001 Information Security Management System and TS EN ISO 9001 Quality Management System certifications shall be conducted by independent, authorized assessor.

TURKTRUST's institutional internal audit is conducted by TURKTRUST's authorized personnel.

8.4. Topics Covered by Assessment

The ETSI 102 042 audit covers all the processes of OV SSL 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 and TS EN ISO 9001 Quality Management System certifications cover TURKTRUST's electronic certification and time-stamping services.

The internal audit covers all matters within the scope of ETSI TS 102 042, ISO/IEC 27001 and TS EN ISO 9001.

8.5. Actions Taken as a Result of Deficiency

TURKTRUST identifies the corrective and preventive actions about the minor non-conformities detected during the ETSI TS 102 042 conformance audit of the OV SSL 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 and TS EN ISO 9001 Quality 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 audit results of OV SSL 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 and TS EN ISO 9001 Quality 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 CPS 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

Server certificates and OSCs issued by TURKTRUST are priced according to certificate type, term and characteristics. Furthermore, during pricing of server certificates, the extent of material transaction limits, the commercial general liability insurance is 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.

Access services on revocation or status information provided by TURKTRUST for server certificates and OSCs are 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

For server certificates and OSCs, 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 commercial general liability insurance in accordance with the ETSI TS 102 042 standard concerning server certificate services.

9.2.1. Insurance Coverage

Server certificates are covered by commercial general liability insurance indicated below.

The commercial general liability insurance covers all direct and indirect damages that can be linked to the server certificate services.

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End-Users

TURKTRUST is under obligation to carry commercial general liability insurance in accordance with the ETSI TS 102 042 standard concerning server certificate 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, standards 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 such customer information as demographic information, communications information not included in the certificate's content is deemed private information.

9.4.3. Information Not Deemed Private

Information included in the certificates of subscribers who are 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 document and subscriber's 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 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. The procedures and instructions related to each process are determined in details to handle those operations accurately and in a complete manner.

As regards to DV SSL ve OV SSL certificates, TURKTRUST specifically warrants that:

- ***Legal Existence:*** TURKTRUST has confirmed that, as of the date the OV SSL certificate was issued, the Subject named in the OV SSL certificate legally exists as a valid organization or entity. This verification is done via documentation provided by, or communication with, a government agency or reliable database of country. In Turkey, this verification is done by Trade Registry Journal, Official Journal or affiliated registry.
- ***Identity:*** TURKTRUST has confirmed that, as of the date the OV SSL certificate was issued, the legal name of the Subject named in the OV SSL certificate matches the name on the official government records. This confirmation is done via reliable database of country.

- ***Right to Use Domain Name:*** TURKTRUST has taken all steps reasonably necessary to verify that, as of the date the server certificate was issued, either the Subject named in the server certificate has the exclusive right to use all the Domain Name(s) listed in the server certificate or had control of, the Domain Name(s) listed in the certificate's subject field and subjectAltName extension. For OV SSL applications this verification is done either by designation of a special web page in the domain name or communication via special e-mail address. For DV SSL applications this verification is done by a communication via special e-mail address. For OV SSL applications this verification can also be done either communicating directly with the national or international domain name registrant or right to use domain name assignment.
- ***Authorization for OV SSL Certificate:*** TURKTRUST has taken all steps reasonably necessary to verify that the Subject named in the OV SSL certificate has authorized the issuance of the OV SSL certificate. This authorization verification is done by either official authorization document or the data which is taken from independent resources and confirmed via telephone or it can be done face to face.
- ***Accuracy of Information:*** TURKTRUST has taken all steps, which are listed below, reasonably necessary to verify that all of the other information in the server certificate is accurate, as of the date the server certificate was issued.
  - ***Domain Name (CN):*** Either by designation of a special web page in the domain name or communication via special e-mail address. Verification can also be done either communicating directly with the national or international domain name registrant or right to use domain name assignment.
  - ***Organization Name (O):*** The legal name of the Subject named in the server certificate matches the name on the official government records.
  - ***Organizational Unit (OU):*** This field is optional. Organizational unit is verified on the application form by the authorized signature. If and when it contains tradename, trademark, address or city information in this field official government records are used so as to complete verification.
  - ***Locality (L):*** Subscriber's locality information that is placed in the server certificate application form matches with official government records.
  - ***State (S):*** This field is optional if and when it contains information that data matches with official government records.
  - ***Country Code (C):*** This field contains the two-letter ISO 3166-1 country code for the country in which the issuer's place of business is located.
  - ***Subject Alternative Name (SAN):*** Each entry contains the Fully-Qualified Domain Name. TURKTRUST confirms that the applicant controls the Fully-Qualified Domain Name or has been granted the right to use it by the domain name registrant.
- ***No Misleading Information:*** While the issuance of the server certificate, TURKTRUST implements a procedure that is mentioned above briefly, 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 the server 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 server certificate as valid or revoked; and
- ***Revocation:*** TURKTRUST follows the requirements of this CPS and revoke the server certificate for any of the revocation reasons specified in the CA/Browser Forum Guidelines.

During the certificate application TURKTRUST declares the binding obligations of the certificate usage by having the SSL subscribers sign the Letter of Commitment By The SSL Subscriber. Issuing certification authority under TURKTRUST fulfills CA obligations stated in the ETSI TS 102 042 and BR obligations to perform server certificate and OSC services.

Besides CP and CPS documents TURKTRUST published the Letter of Commitment By the SSL Subscriber and Letter of Commitment for SSL Services under Repository of www.turktrust.com.tr according to 7 days 24 hours basis.

9.6.2. Registration authority Representations and Warranties

Registration center under TURKTRUST represents 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 letter of commitment.

9.6.4. Relying Party Representations and Warranties

The owners of server 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

Electronic 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 letter of commitment.

For server certificates and OSCs, commercial general liability insurance covers USD 1.000.000 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. In such case, 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 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 CPS Documentation

9.10.1. Term of CP Documentation

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

9.10.2. Termination of CP Documentation

Where a situation arises that require changing the content of the present version of this CPS document depending on changes and arrangements that may occur in 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 CPS version terminates, necessary measures are taken to ensure continuity of TURKTRUST's activities and certification services. The new CPS version is prepared before the validity of the old CPS version terminates and the change shall be realized without interruption of service.

Where it becomes necessary to make changes in certificates issued by 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

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

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 CPS document depending on changes and arrangements that may occur in TURKTRUST's activities and certification services, a new CPS 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 CPS document undergo minor changes that would not affect the use and acceptability of certificates issued earlier, there may be significant changes that would directly affect certificate use. 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 CPS document depending on changes and arrangements that may occur in TURKTRUST's activities and certification services, a new CPS document version which covers relevant changes shall be prepared and published by TURKTRUST.

The CPS document and related practices 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 amendment shall be published in the TURKTRUST website, subscribers shall be notified through e-mail or SMS, and where necessary all relying parties shall be informed through the press media.

Minor changes are announced in the web site.

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 electronic 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.

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

9.14. Governing Law

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

9.15. Compliance with Applicable Law

TURKTRUST provides qualified electronic certificate services in accordance with the "Electronic Signature Law" no.5070 and the Ordinances and Communiqués issued by the Information and Communications Technologies Authority of Turkey.

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 majeure. While such forces majeure 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 majeure.

9.17. Other Provisions

Not applicable.