e-tuğra

CERTIFICATION PRACTICE STATEMENT

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
(E-Tugra EBG Information Technologies and Services Corp.)
Version: 5.1
Validity Date: January, 2022
Update Date: 12/01/2022

Ceyhun Atıf Kansu Cad. 130/58
Balgat / ANKARA
TURKEY

Phone: 90.850.532.23.14
Phone: 90.850.532.23.12
Fax: 90.312.473.56.91
www.e-tugra.com.tr

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-Tugra EBG Information Technologies and Services Corp.) Certification Practice Statement (CPS)

Trademark Notices

CONTENTS

DOCUMENT HISTORY

Version	Release Dates	Status & Description
V4.0	20/06/2016	New format adaptation
V4.1	26/08/2016	Administrative update/ clarifications Yearly
V4.2	29/09/2017	Administrative update/ clarifications Yearly
V4.3	26/01/2018	ETSI 319-411x Adaptation BR Requirements Changes Administrative update/ clarifications Yearly
V4.4	29/08/2018	Administrative update/ clarifications Yearly BR Requirements Changes Roots Info were added
V4.5	21/10/2019	Certificate Chains Added. Reseller Section was added Certificate Hierarchy was added CAB Forum documents versions are updated Region restriction for Certificate Application were updated CRL and OCSP update routines updated.
V4.6	30/03/2020	New Roots added Administrative update/ clarifications Yearly Upgrades with Mozilla Policy Review
V4.7	12/03/2021	Enhancement on Revocation Process Revocation Contact Person Subordinates Usages BR Requirements Checks
V4.8	05/07/2021	Updates to section 4.9.12 to reflect Mozilla 2.7.1 updates for private key compromise. Revision on Authentication of Domain Names Revision on Life Cycle Technical Controls Fixing wording mistakes
V4.9	20/08/2021	Update on compliance documents versions
V5.0	25/10/2021	Update on Certificate Policies
v5.1	12/01/2022	Updates and improvements for Root Inclusion on Bugzilla 1628720 Major changes: * Revocation procedures revised, * Remove misunderstanding on certificate profiles & policy identifiers, * Corrections on Name Forms, Certificates extensions, Uniqueness of Names and Certificate Profiles. * Web addresses and contacts, * Verifications resources for organizations QIIS, QGIS etc. * Handling IDN domain names, * Required skills and qualification of Contractors, * Improvement on Private Key Compromise Procedures, * EV Verification improvements according to EVG

1. INTRODUCTION

EBG Bilişim Teknolojileri ve Hizmetleri AŞ (EBG Information Technologies and Services Corp. To be referred to as “e-tuğra hereafter) is a joint stock company (AŞ), which is incorporated and presently continues operations in compliance with the Turkish Commercial Code. It has obtained the right and powers of providing services related to electronic signatures, electronic certificates both QEC and NQC and time stamps in its capacity as an Electronic Certificate Service Provider (to be referred “ECSP” hereafter) after it has made a notification to the Telecommunication Agency and met the legal requirements in accordance with Article 8 of Law No 5070 on Electronic Signatures.

This document entitled Certification Practice Statement (to be referred to as “CPS” hereafter) has been prepared for the purpose of explaining and making public the technical and legal requirements met by e-tuğra in its capacity as an “ECSP”, its operations, its technical and organizational structure and obligations of the parties assuming certain roles in connection with services provided by “ECSP”.

This document identifies the practice statements in the operations such as certificate applications, certificate issuance and management of certificates, certificate renewal and certificate revocation to be conducted in compliance with administrative, technical and legal requirements; it also sets the implementing responsibilities of e-tuğra as an ECSP, of the certificate owner and of the third parties.

This document has been prepared in order to show the operations of e-tuğra as an electronic certificate service provider in compliance with:

- The standards of ETSI TS 101 456, of IEF RFC 3647 and of CWA 14167-2, CWA 14167-3, CWA 14167-4 required by the Law No 5070 on Electronic Signatures (briefly “the Law”), the Regulation on the Procedures and Principles Applicable for Implementation of the Electronic Signatures Law (briefly “the Regulation”) and the Communiqué on the Process and Technical Criteria Applicable for the Electronic Signatures (briefly “the Communiqué”).
- The documents published at http://www.CAB Forum.org by “CA/Browser Forum” which are called “Guidelines for Issuance and Management of Extended Validation Certificates”, Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates” and “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” for the services such as Standard (DV) SSL (Secure Socket Layer), Premium (OV) SSL, EV (Extended Validation) SSL Certificates and Code Signing Certificate.
- For Code Signing Certificates Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, published at https://aka.ms/csbr (the “Code Signing Minimum Requirements”) for Code Signing Certificates are applied.
- For SSL and Code Signing Certificates, ETSI EN 319 411-1 and related ETSI EN 319 401 are applicable. The policies Normalized Certificate Policy, Domain Validated Certificate Policy, Organization Validated Certificate Policy, Extended Validated Certificate Policy and Extended Validated Certificate Guideless in ETSI EN 319 411-1 are applied.

If there is a conflict between one of these documents above and this CPS, the Requirements of CAB Forum and ETSI take precedence over this document.

1.1. Overview

"e-tuğra" is an "Electronic Certificate Service Provider" authorized by "Information and Communication Technologies Authority". It has gained this right after fulfilling the necessary requirements in related laws and regulations.

"e-tuğra" publicly discloses and brings to the attention of the parties the features of the electronic certificates and the considerations governing their use, certification processes, rights and obligations of the parties taking part in the certification process and the technical and operational activities that it carries out in its capacity as "CSP" under the document of Certificate Policy "CP". In addition, "e-tuğra" outlines how the aspects covered by "CP" are implemented in the document called "Certification Practice Statement" (to be referred as "CPS" hereafter) and it brings this document to the attention of the public and the concerned parties. Principles in this document cover e-tuğra's customer services, registration units, certificate issuance procedures which in turn all of e-tuğra's electronic certificate services.

"e-tuğra" conducts electronic certification services according to the practice statement in "CPS" and procedures and instructions of ISO/IEC 27001 Information Security Management System and auxiliary guides.

1.2. Document Name and Identification

This "CPS" document is called "e-tuğra Certification Practice Statement" and it is prepared in order to explain the certification practice statement. The version number and the validity date take place on the cover page of the document.

"e-tuğra CPS document", describes how "e-tuğra" runs the activities on certification services related to certificate policies defined in "e-tuğra CP document. "e-tuğra CPS document", includes the practice statement of object identifiers (OIDs) of all certificate types defined in "e-tuğra CP document" and they are given below.

E-tuğra's "CPS", by the use of the corporate object identifier "2.16.792.3.0.4" taken from Turkish Standards Institution by e-signs, covers all of the following certificate policies.

This document is disclosed to the public at the website http://www.e-tugra.com.tr.

"e-tuğra" Qualified Electronic Certificate Policy
It covers qualified electronic certificates which allow the use of secure electronic signatures equivalent to hand written signatures of individuals according to the Law no 5070, the regulation and the Communiqué.
Object Identifier: 2.16.792.3.0.4.1.1.1

"e-tuğra" Standard (DV) SSL Certificate Policy,
It covers Domain Validated SSL certificates for servers based on CAB Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".
Object Identifier: 2.16.792.3.0.4.1.1.2

* Corresponds to policy with OID: 0.4.0.2042.1.6 ETSI 319 411-1 DVCP
* Corresponds to policy with OID: 2.23.140.1.2.1 CAB Forum BR Guide

"e-tuğra" Premium (OV) SSL Certificate Policy,

It covers Organizational Validated SSL certificates for servers based on CAB Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

Object Identifier: 2.16.792.3.0.4.1.1.3

* Corresponds to policy with OID: 0.4.0.2042.1.7 ETSI 319 411-1 OVCP
* Corresponds to policy with OID: 2.23.140.1.2.2 CAB Forum BR Guide

"e-tuğra" EV SSL Certificate Policy,

It covers Extended Validated (EV) SSL certificates for servers based on CAB Forum "Guidelines for Issuance and Management of Extended Validation Certificates".

Object Identifier: 2.16.792.3.0.4.1.1.4

* Corresponds to policy with OID: 0.4.0.2042.1.4 ETSI 319 411-1 EVCP
* Corresponds to policy with OID: 2.23.140.1.1 CAB Forum EV Guide

"e-tuğra" Code Signing Certificate Policy,

It covers the Organization Validated Code Signing Certificates.

Object Identifier: 2.16.792.3.0.4.1.1.13

* Corresponds to policy with OID: 0.4.0.2042.1.7 ETSI 319 411-1 OCVP
* Corresponds to policy with OID: 2.23.140.1.4.1 CAB Forum CS Guide

"e-tuğra" EV Code Signing Certificate Policy,

It covers the Extended Validated (EV) Code Signing certificates for code signing operations.

Object Identifier: 2.16.792.3.0.4.1.1.14

* Corresponds to policy with OID: 0.4.0.2042.1.4 ETSI 319 411-1 EVCP and EVCG
* Corresponds to policy with OID: 2.23.140.1.3 CAB Forum EVCS Guide

1.3. Participants

The subjects defined as Participants under "e-tuğra CPS" are the parties which take part in e-tuğra's operations as "ECSP" and hold the rights and obligations with regard to such operations.

The participants under "e-tuğra CPS" are e-tuğra as Electronic Certificate Service Provider (ECSP), registration authorities, individual or corporate certificate owners and third parties.

1.3.1. Electronic Certificate Service Provider ("e-tuğra")

e-tuğra is an "ECSP" for which rights and obligations are established in line with the Electronic Signature Law No 5070 and the related legal provisions and this "CPS" document. e-tuğra is responsible for carrying out the operations such as receiving, issuing, distributing, publishing of certificates and the revocation, renewal of the certificates and the services related to all Private Key Infrastructure like OCSP and CRL. All these operations are conducted by the "Trust Center" which takes place at e-tuğra's center.

End user certificates are issued by e-tuğra as "ECSP" and are signed by e-tuğra intermediate CAs.

All intermediate CAs are issued by e-tuğra as "ECSP" according to their key usage areas and are signed by e-tuğra root CA.

1.3.2. Registration Authorities

Registration Authorities (to be referred to as "RA" hereafter) are the residential structures which perform services related to the application, renewal or revocation of certificate requests and which

are under direct control and inspection of e-tuğra and the staff affiliated to e-tuğra, employed whether directly or on contract or outsourced in these residential structures or individual people and/or corporate entities which conclude Registration Unit Contracts by e-tuğra.

On the basis of documents established by e-tuğra, RAs are responsible for checking the identification of Certificate Holders applying for certificate and the validity of the information to be incorporated in certificates. In addition, RAs can also assume responsibilities for receiving applications for operations to be carried out between "Certificate Holders" and e-tuğra throughout the certificate life cycle and for performing necessary operations for and on behalf of e-tuğra.

Certificate applications to be made via RAs can be realized by direct visit of the applicant to the RA's office and necessary information and documents delivered to the office by the applicant or posted by mail according to e-tuğra application process procedures. In either way certificate requests are forwarded to e-tuğra's Trust Center and the certificates are issued.

For qualified electronic certificates (QECs), "RAs" may also conduct application procedures about "secure e-signature package" which consists of various equipment's and services related to the operations of e-tuğra such as minimum secure electronic signature developing tool and qualified electronic certificate on behalf of e-tuğra. "RAs" which have necessary safety measures may also fulfill the duty of issuing electronic signature function for the qualified certificate applications which completed all necessary approvals.

"e-tuğra" does not delegate domain validation for SSL certificates to RAs

The address and communication information of all RAs are disclosed to the public via the website of "e-tuğra".

1.3.3. Certificate Owners

Certificate owners are those people or organizations whose identity or title is verified in order for the certificates to be issued for them.

Verification of identity and /or title depends on the type of certificate to be applied according to the related regulations and standards. The verification procedures of identity and/or title are explained in the 3rd section.

The liability of the certificate owner and consequences due to the use of a certificate are determined by the relevant legislation and the certificate owner's commitment or agreement.

According to the No 5070 Electronic Signature Law, qualified electronic certificates (QECs) are issued only for natural persons by "ECSPs". Qualified certificate owner is the natural person who fulfills the requirements cited in e-tuğra's "CP" and "CPS" documents and in "Qualified Certificate Owner User Agreement" and whose certificate is issued. Application for qualified electronic certificates can be done in two ways;

Individual applicant is the natural person who applies for himself and signs the QEC User Agreement with e-tuğra after having met the required procedures. Moreover, if individual applicants deliver the required official documents to e-tuğra during the application process they can assure the professional information and the related information they are affiliated with to be featured appropriately according to the standards.

Corporate applicants are the legal entities which apply for QEC for and on behalf of its employees or customers or members or shareholders and sign a Corporate Application Form with e-tuğra after having met the required procedures.

1.3.4. Resellers

Resellers are only responsible for marketing and sales of e-tuğra certificates with a given rights and region restriction. All certificate applications done via resellers are validated and processed by e-tuğra or Registration Authorities of e-tuğra. For other trademark sub CA's created for issuing standard and Premium (OV) SSL other than e-tuğra, the owners of trademarks have only sales and marketing rights for these trademarks. All validation of applications and issuing of certificates for all Sub-CA are only done by e-tuğra.

1.3.5. Third Parties

Third parties are those who receive documents signed by private keys based on the certificates issued by e-tuğra and those who rely on the relevant certificates.

Third parties are those who verify the identity of the person signing the data signed by owned private keys by using QECs; those who control the validity of e-tuğra's root and intermediate certificates and those who conduct business, make transactions relying on the data signed by private keys of e-tuğra certificates.

QEC holders act as third parties in case they directly fulfill the verification processes mentioned above.

The limits of the liability of e-tuğra to third parties are stated in this "CPS" document.

1.3.6. Other Parties

In the context of all certification services such as certificate issuing, publication of repository and the preservation of the security of the certificate information are provided by e-tuğra.

Other parties are the individuals or corporate institutions which cooperate with e-tuğra and provide service.

E-tuğra signs contracts with other parties in order to guarantee that the service given by them are reliable and proper, business processes are conducted according to the procedures and instructions required by this "CPS" prepared by e-tuğra and that any private or confidential information about certificate owners are not disclosed

1.4. Certificate Usage

1.4.1. Use of Authorized Certificates

"e-tuğra" root and intermediate certificates can only be used to sign certificates in accordance with the purpose of use and to verify data and certificates.

QECs issued by e-tuğra can only be used as part of the processes of creating and verifying secure electronic signatures in the framework of limitations incorporated in the certificates concerning usage and material scope and in line with QEC User Agreement. QECs are used for signing forms and documents in e-government, e-commerce and similar practices; signing all kinds of commercial and official documents electronically; verifying identity in all network environments that require identification and authentication. QECs can also be used by third parties for purposes of validating effectiveness of certificates and gaining access to certificate contents.

All SSL certificates are used by certificate owners on servers only for the domain names in the certificate and for SSL operations.

SSL Certificates;

- Standard (DV) SSL: It verifies a Domain Name and the identity of the web services on this Domain Name and it guarantees that the communication is encrypted.
- Premium (OV) SSL: It verifies a Domain Name and the identity of the associated institution, and it also guarantees that the communication with web services on this domain name to be encrypted.
- EV SSL: It verifies a Domain Name and the identity of the associated institution, and it also guarantees that the communication with web services on this domain to be encrypted. e-tuğra makes sure that the relation between the EV SSL Certificate Domain Name and the institution to be in line with the "Guidelines for Issuance and Management of Extended Validation Certificates" published by "CA/Browser Forum" and it develops the certificate.

Code Signing Certificate (CSC) is used for signing software codes by the real person and/or institution which holds the intellectual property rights of certificate owners.

The usage rights of all certificates belong only to certificate owners.

1.4.2. Prohibited Usage of Certificates

It is prohibited to use root and intermediate certificates issued by e-tuğra for purposes other than determined conditions in the regulations.

The use of QECs issued by e-tuğra for creating electronic signatures and for verifying processes is prohibited in restricted operations by Electronic Signature Law. QECs cannot be used for purposes other than established by regulations.

The right of usage of all other e-tuğra certificates belongs to certificate owners and the use of certificates beyond the control of the certificate owner is not allowed.

e-tuğra certificates cannot be used outside the limits and scope declared in this "CPS" document.

1.4.3. Certificate Hierarchy

The Root CA's and the Sub-CAs that have been issued by the mentioned Root-CA's below are subject to practices in this document.

1.4.3.1 Certification Authorities and Subordinates

Identification of the Root-CA:	E-Tugra certification Authority
Distinguished Name	CN=E-Tugra Certification Authority, OU=E-Tugra Sertifikasyon Merkezi, O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., L=Ankara, C=TR
SHA-256 fingerprint	B0:BF:D5:2B:B0:D7:D9:BD:92:BF:5D:4D:C1:3D:A2:55:C0:2C:54:2F:37:83:65:EA:89:39:11:F5:5E:55:F2:3C
Certificate Serial number	6A683E9C519BCB53

Iden. of the Sub-CA	**Distinguished Name**	**SHA-256 fingerprint**	**Serial number**	**Usage Purpose on End Entities**

E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı v2	CN = E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı v2,OU = E-Tuğra Sertifikasyon Merkezi ,O = E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.L = Ankara,C = TR	DD:2C:B2:EE:C5:2F:5E:96:AB:1C:B8:43:09:52:FB:56:C8:E6:AB:DF:F2:1E:AC:D7:68:4B:1C:D7:38:AA:CC:FF	1F0EC403B3801CAD	(Qualified Signature Purpose)
E-Tugra Domain Validated CA	CN=E-Tugra Domain Validated CA,OU=E-Tuğra Sertifikasyon Merkezi,O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.,L=Ankara,C=TR	CB:6F:CE:E4:1C:55:E2:47:74:DF:02:BE:35:DE:6D:41:8E:94:EF:58:11:F7:DB:13:73:AF:88:09:CF:70:7F:2A	3AEFB1B7FA55ADC0	TLS Web Server Authentication, TLS Web Client Authentication
E-Tugra Extended Validated CA	CN=E-Tugra Extended Validated CA,OU=E-Tuğra Sertifikasyon Merkezi,O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.,L=Ankara,C=TR	CE:7A:DC:19:77:57:A5:2E:69:A2:01:4C:CE:03:D9:80:63:25:02:76:47:42:C2:92:3D:73:80:56:8E:21:00:A6	7815C206C403B277	TLS Web Server Authentication, TLS Web Client Authentication, Code Signing
E-Tugra Organization Validated CA	CN=E-Tugra Organization Validated CA,OU=E-Tuğra Sertifikasyon Merkezi,O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.,L=Ankara,C=TR	11:47:53:E8:8D:00:0E:75:99:61:5A:99:07:E2:6B:73:B6:D8:51:31:7F:F2:B2:7A:CA:9D:B8:FC:50:56:92:A7	60D6C12084607AF0	TLS Web Server Authentication, TLS Web Client Authentication, Code Signing
TrustSafe Domain Validated CA	CN=TrustSafe Domain Validated CA,OU=SSL Department,O=Isimtescil Bilisim Anonim Sirketi,L=Istanbul,C=TR	50:AA:20:D9:BE:BB:6D:22:4E:4F:A7:72:CE:B9:01:CA:7B:84:DE:54:5A:0F:4E:F9:4D:BC:E1:AC:41:F7:D0:0D	5A1BDFDCB9826A12	TLS Web Server Authentication, TLS Web Client Authentication
TrustSafe Organization Validated CA	CN=TrustSafe Organization Validated CAOU=SSL Department,O=Isimtescil Bilisim Anonim Sirketi,L=Istanbul,C=TR	C2:B8:70:C3:85:C8:C8:25:0F:2D:50:9A:11:76:4A:3C:13:8D:2A:02:56:6F:36:1C:09:96:AB:CC:8A:00:B3:6A	2CB328C9D86A55C3	TLS Web Server Authentication, TLS Web Client Authentication

Identification of the Root-CA:	E-Tugra Certification Authority Root NES RSA v3			
Distinguished Name	CN = E-Tugra Certification Authority Root NES RSA v3 OU = E-Tugra Sertifikasyon Merkezi O = E-Tugra EBG A.S. L = Ankara C = TR			
SHA-256 fingerprint	F0:72:2F:1B:0B:A2:DA:29:C6:A7:EE:AF:91:20:54:C5:56:C6:06:AC:1B:95:B7:45:32:AC:7F:81:B9:2D:F6:9E			
Certificate Serial number	40:5B:DE:ED:02:03:E8:D7:AC:6E:53:A1:0E:5B:EF:A5:33:C7:4E:92			
Iden. of the Sub-CA	**Distinguished Name**	**SHA-256 fingerprint**	**Serial number**	**Usage Purpose on End Entities**

E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı RSA v3	CN = E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı RSA v3,OU=E-Tuğra Sertifikasyon Merkezi,O=E-Tuğra EBG A.Ş.,L=Ankara,C=TR	24:72:5D:37:5D:59:0B:83:6F:B4:36:B8:81:10:57:6E:3F:D9:26:26:47:7E:EF:36:EC:D6:E0:EB:68:53:6D:68	30:F8:23:9C:14:F1:D9:9E:03:3E:CC:DB:70:F9:F2:C7:38:11:15:EA	(Qualified Signature Purpose)

Identification of the Root-CA:	E-Tugra Certification Authority Root NES ECC v3			
Distinguished Name	CN = E-Tugra Certification Authority Root NES ECC v3 OU = E-Tugra Sertifikasyon Merkezi O = E-Tugra EBG A.S. L = Ankara C = TR			
SHA-256 fingerprint	1C:B8:DF:3E:F2:44:B4:7C:BB:99:CC:5D:A8:26:B1:BD:67:34:59:F2:2C:B7:84:D2:3C:70:C9:5E:67:72:CF:D4			
Certificate Serial number	62:8D:9B:69:79:D1:64:83:6D:FF:C8:27:AE:42:6D:92:6A:50:DF:94			
Iden. of the Sub-CA	**Distinguished Name**	**SHA-256 fingerprint**	**Serial number**	**Usage Purpose on End Entities**
E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı ECC v3	CN = E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı ECC v3,OU = E-Tuğra Sertifikasyon Merkezi,O = E-Tuğra EBG A.Ş.,L = Ankara,C = TR	93:0B:9C:7E:43:17:EC:1D:43:6A:64:EB:32:C5:54:AE:B2:86:FC:60:49:B2:F2:33:D6:60:7F:64:15:28:A0:2A	5C:0B:72:EC:33:AC:6F:B9:0A:28:EB:06:1D:3F:DC:16:D4:21:46:66	(Qualified Signature Purpose)

Identification of the Root-CA:	E-Tugra Global Root CA RSA v3			
Distinguished Name	CN = E-Tugra Global Root CA RSA v3 OU = E-Tugra Trust Center O = E-Tugra EBG A.S. L = Ankara C = TR			
SHA-256 fingerprint	EF:66:B0:B1:0A:3C:DB:9F:2E:36:48:C7:6B:D2:AF:18:EA:D2:BF:E6:F1:17:65:5E:28:C4:06:0D:A1:A3:F4:C2			
Certificate Serial number	0D:4D:C5:CD:16:22:95:96:08:7E:B8:0B:7F:15:06:34:FB:79:10:34			
Iden. of the Sub-CA	**Distinguished Name**	**SHA-256 fingerprint**	**Serial number**	**Usage Purpose on End Entities**

E-Tugra Extended Validated CA RSA v3	CN = E-Tugra Extended Validated CA RSA v3,OU = E-Tugra Trust Center,O = E-Tugra EBG A.S.,L = Ankara,C = TR	5F:4F:81:D8:85:65:3A:50:3A:9E:4D:23:56:19:49:BE:ED:9A:5B:72:34:98:5E:EC:23:00:20:BE:3D:79:1A:81	31:38:FF:98:B1:AC:CC:72:BD:FB:C6:5D:2B:D8:CB:C8:3F:35:FE:CF	Client Authentication, Server Authentication
E-Tugra Organization Validated CA RSA v3	CN = E-Tugra Organization Validated CA RSA v3,OU = E-Tugra Trust Center,O = E-Tugra EBG A.S.,L = Ankara,C = TR	D4:C4:CA:F9:A1:B2:E2:0A:AF:77:E9:39:51:EF:B6:97:3A:3B:AC:9D:26:1D:67:46:AA:C4:A4:9E:07:85:AA:DD	55:E1:B4:43:9D:B2:A1:B7:12:13:48:D6:35:AA:77:12:B6:DF:42:B4	Client Authentication, Server Authentication
E-Tugra Domain Validated CA RSA v3	CN = E-Tugra Domain Validated CA RSA v3,OU = E-Tugra Trust Center,O = E-Tugra EBG A.S.,L = Ankara,C = TR	9D:C9:46:CD:46:62:BE:72:B3:59:70:50:EE:3A:31:7D:83:7A:CC:7C:0F:CE:51:54:D4:68:85:E0:FE:F4:89:39	49:28:FE:65:65:97:40:8D:4D:7A:24:2C:2E:91:BB:E7:FD:CB:0B:D7	Client Authentication, Server Authentication

Identification of the Root-CA:	E-Tugra Global Root CA ECC v3
Distinguished Name	CN = E-Tugra Global Root CA ECC v3 OU = E-Tugra Trust Center O = E-Tugra EBG A.S. L = Ankara C = TR
SHA-256 fingerprint	87:3F:46:85:FA:7F:56:36:25:25:2E:6D:36:BC:D7:F1:6F:C2:49:51:F2:64:E4:7E:1B:95:4F:49:08:CD:CA:13
Certificate Serial number	26:46:19:77:31:E1:4F:6F:28:36:DE:39:51:86:E6:D4:97:88:22:C1

Iden. of the Sub-CA	**Distinguished Name**	**SHA-256 fingerprint**	**Serial number**	**Usage Purpose on End Entities**
E-Tugra Extended Validated CA ECC v3	CN = E-Tugra Extended Validated CA ECC v3,OU = E-Tugra Trust Center,O = E-Tugra EBG A.S.,L = Ankara,C = TR	80:D5:4E:E5:4C:A5:64:8C:0E:A1:4F:A5:DF:95:35:CA:53:61:55:CE:90:02:67:CB:E9:AC:B3:9E:18:2E:DC:59	7B:F1:81:E3:25:1F:AB:B7:4C:B8:52:A9:53:62:81:78:DD:7D:D1:94	Client Authentication, Server Authentication
E-Tugra Organization Validated CA ECC v3	CN = E-Tugra Organization Validated CA ECC v3,OU = E-Tugra Trust Center,O = E-Tugra EBG A.S.,L = Ankara,C = TR	87:EC:80:B7:06:20:53:FE:5A:CD:4A:BE:84:B0:1E:BF:34:04:A6:4C:6B:27:CE:AB:53:1E:A7:50:90:AA:43:F1	15:53:3C:F8:96:7C:68:15:1E:89:AA:38:86:BF:4B:92:7E:3E:16:7E	Client Authentication, Server Authentication
E-Tugra Domain Validated CA ECC v3	CN = E-Tugra Domain Validated CA ECC v3 OU = E-Tugra Trust Center O = E-Tugra EBG A.S. L = Ankara C = TR	51:10:1F:AA:96:31:29:31:9A:4A:07:75:3F:B3:BA:D3:90:1C:BA:CF:6F:19:03:9F:A0:E0:56:35:AF:AD:58:FC	4F:EE:B0:CC:9B:2B:77:DB:54:20:CD:4D:64:75:09:E3:B3:B3:2A:DE	- Client Authentication, Server Authentication

1.5. Policy Administration

e-tuğra, as the authority that establishes the certificate policy is responsible for the management of the “CP” document to which this “CPS” document is subordinate.

1.5.1. Organization Administering the Document

The security forum formed by e-tuğra staff which is specifically authorized by e-tuğra is responsible for publication, revision, renewal and all related operations of “CPS” documents. All rights and responsibilities associated with this document belong to e-tuğra.

1.5.2. Contact

Contact information for e-tuğra “CPS” follows;
E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-Tuğra EBG Information Technologies and Services Corp.).
Address: Ceyhun Atıf Kansu Cad. Gözde Plaza No:130/58-59 Balgat Ankara
Phone: 0-312-473 56 90
Fax: 0-312-473 56 91
Call Center: 0-850-532 23 14
Technical Support: 0-850-532 23 12
E-Mail: info@e-tugra.com.tr , destek@e-tugra.com.tr
Web: http://www.e-tugra.com.tr – http://www.e-tugra.com

Revocation Reporting Contact Information

Address: Ceyhun Atıf Kansu Cad. Gözde Plaza No:130/58-59 Balgat Ankara
Technical Support: 0-850-532 23 12
E-Mail: revoke@e-tugra.com.tr , iptal@e-tugra.com.tr
Web: http://www.e-tugra.com.tr – https://helpdesk.e-tugra.com.tr/submit_ticket

1.5.3. Person Determining CPS Suitability for the Policy

The compatibility of this CPS document to the CP and to e-tuğra ECSP certificate processes is audited by authorized e-tuğra “trusted staff” and e-tuğra management board.

1.5.4. “CPS” approval procedures

“e-tuğra” authorities conduct audit operations on a regular basis for "CPS" document and for “e-tuğra” "ECSP" processes. In accordance with the audit outcomes and/or in case of modification on “ECSP” operational processes, modification or renewal is done on “CPS”. "CPS" changes or new version is submitted to the competent “e-tuğra” security forum and the senior management of security.

Before publishing new versions of CP and CPS to the public, they are submitted for Information Technologies and Telecommunications Authority’s review.

The senior management and security board of “e-tuğra” is responsible for ensuring whether the certification practices established to meet the applicable requirements specified in this CPS are properly implemented.

1.6. Definitions and Acronyms

1.6.1. Abbreviations

Abbreviation	Explanation/Definition
"BTK"	Bilgi Teknolojileri ve İletişim Kurumu (Information and Communication Technologies Authority)
"CEN"	Comité Européen de Normalisation
"CP"	Certificate Policies
"CPS"	Certification Practice Statement
"CRL"	Certificate Revocation List
"CSR"	Certificate Signing Request
"CSC"	Code Signing Certificate
"CWA"	CEN Workshop Agreement
"DN"	Distinguished Name
"DNS"	Domain Name System
“DVCP”	Domain Validation Certificate Policy
"EAL"	Evaluation Assurance Level
"ECSP"	Electronic Certificate Service Provider
"ETSI TS"	ETSI Technical Specifications
"ETSI"	European Telecommunication Standardization Institute
“e-tuğra”	E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
"EV"	Extended Validation
“EVG”	Extended Validation Guidelines
“EVCP”	Extended Validation Certificate Policy
“EVCG”	Extended Validation Certificate Policy Guideless
"DRC"	Disaster Recovery Center
“IDN”	Internationalized Domain Name
“DBA”	Doing Business As
"IETF RFC"	Internet Engineering Task Force Request for Comments
"IETF"	Internet Engineering Task Force
"ISO/IEC"	International Organization for Standardization / International Electrotechnical Committee
“NCP”	Normalized Certificate Policy
"RA"	Registered Authority
"QEC"	Qualified Electronic Certificate
"OCSP"	Online Certificate Status Protocol
"OID"	Object Identifier.
“OVCP”	“Organization Validation Certificate Policy”
"PKI"	Public-Key Infrastructure
"SSL"	Secure Sockets Layer
"TC"	Republic of Turkey
"TCKN"	Republic of Turkey the Number of Citizenship
"TSE"	Turkish Standards Institution

1.6.2. Definitions

Concept	Explanation/Definition

"Activation Password"	The passwords to access secure signature creation devices.
"Activation"	An alternative and secure method that allows QEC subscribers to create and define the activation data of their QEC via secure online application, themselves.
"Application Methods"	Methods comprising of technical and administrative processes by which an application is made by QEC Applicants to "ECSP", necessary documents are drawn up, certificate charges are paid, documents are retained, and qualified electronic certificates are issued and forwarded to certificate owners and aspects such as the procedures over the communication of requests for Revocation, renewal and suspension of certificates. These methods are available at www.e-tugra.com.tr.
"Archive"	All information, documents and electronic data that ECSP has to keep
"Authority" - "Agency" - "Institution"	Information Technologies and Telecommunications Authority
"Certificate Holder" - "Certificate Owner" - "Certificate User"	Natural person or legal entity for which a certificate is issued by ECSP. "Certificate Holder", "Certificate Owner" and "Certificate User" used in this document have synonymous meaning.
"Certificate policy"	Rules as a whole which designate the acceptability of certificates in view of implementations which are a certain gathering of security requirements and/or a group of general requirements are called "Certificate policy". "Certificate policy" is a document made public by electronic certificate service providers, which aim at meeting the objectives outlined above. Certificate users have to comply with CP published by "ECSP". CP including any changes thereto which may be introduced from time to time is available on "ECSP" web site.
"Certificate Practice Statement "	It is a public statement made by "ECSP", which is periodically updated, whereby the requirements which have to be met by each party defined as part of ECPS, particularly Certificate Users, in order to achieve designated operations and whereby implementations and procedures are elaborated. CPS including any changes that may be made thereto periodically is available on "ECSP" web site.
"Certificate Revocation List"	An electronic file that has been generated, signed and published by the ECSP 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.
"Code Signing Certificate" ("CSC")	The certificate that verifies the owner of the source code of software that can be executed on a computer.
"Communiqué"	"Communiqué on the Processes and Technical Criteria Applicable for Electronic Signatures", which was promulgated in the Official Journal Issue No 25692 of January 6, 2005.
"Corporate Applicant"	Legal entity with which a Corporate Application Contract is concluded with "ECSP" and which applies for qualified electronic certificates for its employees or customers or members or shareholders pursuant to Articles 3 and 9 of the Regulation.
"Corporate Application Officer"	An employee of the Corporate Applicant, who determines the information to be notified to "ECSP" for issuance of QEC of Certificate User by relying on documents indicated by Article 9/1 of the Regulation and fulfills all the obligations of the "Corporate Application Contract" for and on behalf of the Corporate Applicant.

"Corporate Application"	Application made by a legal entity for qualified electronic certificates for its employees or customers or members or shareholders.
"Directory"	An electronic storage which includes valid certificates.
"Distinguished Name Field" ("DN")	Field that consists of either the subscriber's or the issuer's name on the certificate. It may comprise of different subfields like CN, O, OU, T, L and SERIALNUMBER, each of which may exist with the relaxant data depending on the type of certificate.
"Electronic Certificate Service Provider"	A public agency or institution or natural or legal persons in private law authorized to provide electronic certification, time-stamping and electronic signature services.
"Electronic Data"	Records generated, transported or stored in electronic, optical or similar means.
"Electronic Signature Law"	Law no. 5070 published in the official journal on 15 January 2004.
"Electronic Signature"	Electronic data affixed to other electronic data or having logical association with electronic data and used to authenticate the identification.
"EV SSL"	The SSL certificate issued and maintained in accordance with the "Extended Validity Certificate Policy" defined in ETSI EN 319 411-1 standard and "Guidelines for Issuance and Management of Extended Validation Certificates" published by "CA/Browser Forum".
"Financial Liability Insurance"	Insurance that the ECSP should carry to cover the damages that would arise from its failure to perform its obligations under the Law.
"Hashing Algorithm"	An algorithm which is used to produce a fixed length summary of the electronic data to be signed.
"Identification Info"	Certificate User Name of the Person of the TCKN for citizenships of Turkey, passport number, place of birth, date of birth and nationality for others.
"Intermediate Certificate" ("Sub-root Certificate")	Certificate that has been created for the issuing end user certificates, "Trust Center" pursuant to the PKI hierarchy of the ECSP, carries the signature of the ECSP's root certificate and is used to sign the end user certificates.
"Key"	Any of the public or private keys.
"Law"	Electronic Signature Law published in the official journal on 15 January 2004.
"On-line Certificate Status Protocol" ("OCSP"):	Standard protocol that has been created to disclose the validity status of certificates to the public and allows receipt of certificate status information by on-line methods instantly and without interruption.
"Premium (OV) SSL"	The SSL certificate issued and maintained in accordance with OVCP in ETSI EN 319 411-1 standard and "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by "CA/Browser Forum" and verifies domain names and organization validity.
"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.
"Private Key"	Data such as passwords, cryptographic private keys etc. which are unique, owned and used by the subject to generate an electronic signature; named as signature creation data in the Law.

"Public Key"	Cryptographic key disclosed to the third parties in a public key encryption scheme; named as signature verification data in the Law.
"Qualified Electronic Certificate" ("QEC")	Electronic certificate, which is defined by Article 9 of Law No 5070 in terms of contents and by Article 5 of the Communiqué on the Procedures and Technical Criteria Applicable for Electronic Signatures in terms of technical considerations.
"Registration Authority"	A unit which is included in the ECSP structure, receives certificate applications of certificate subscribers or corporate applicants, and renewal applications, executes identification, verification and authentication processes, approves certificate requests and directs to the issuing "Trust Center", has subunits that handle customer relations under the ECSP activities.
"Regulation"	"Regulation on the Procedures and Principles Applicable for Implementation of the Electronic Signatures Law" which was issued in the Official Journal Issue No 25692 of January 6, 2005.
"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 ECSP's institutional identity information with the ECSP's public key data, has been generated by the issuing "Trust Center", carries its signature, published by the ECSP to verify all certificates issued by the ECSP.
"Secure Electronic Signature Creation Tool"	Secure Electronic Signature Creation tools are the tools at the level of minimum EAL4+ according to ISO / IEC 15408 (-1, -2 and –3) which ensure: a) That the electronic Signature Creation data they produce are unique, b) That the electronic signature formation data recorded on them are never taken out of the tools and that their confidentiality is maintained, c) That the electronic signature formation data recorded on them cannot be retrieved and used by third Parties and that they are protected against electronic signature fraudulency, d) That the data to be signed cannot be changed by any persons other than the signature owners and that such data can be viewed by the signature owners prior to creation of signatures.
"Secure Electronic Signature Verification Tool"	Secure electronic signature verification tools are CWA 14171 standard compliant signature verification tools: a) which show the data used for verification of signature to the person performing validation without changing them, b) which activate the signature validation operation in a reliable and definite manner and show the validation results to the person performing validation without changing them, c) which provide viewing of the signed data in a reliable manner when required, d) which establish the correctness and validity of electronic certificates used for verification of signatures in a reliable manner and show the results thereof to the persons performing validation without changing them,

	e) which show the ID of the signature owner to the person performing validation without making any changes, f) Which provides establishment of any changes which will affect the conditions related to the verification of signatures.
"Secure Electronic Signature"	Secure electronic signature is an electronic signature; a) which is exclusively owned by its holder, b) which is developed only by the secure electronic Signature Creation Tool solely available to the signature owner, c) which provides establishment of the identity of the signature owner on the basis of qualified electronic certificate, d) Which provides determination if any changes have later been made to the signed electronic data.
"Secure e-signature package"	A whole of services and equipment provided by "ECSP" to Certificate Users, which comprises qualified electronic certificates and secure electronic Signature Creation tools as a minimum. Detailed information is available at www.etugra.com.tr on the prices of "Secure e-signature Package" and the equipment and services contained.
"Secure Sockets Layer" ("SSL")	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.
"Signature Creation Tool"	Software or hardware tool that uses the signature creation data to create an electronic signature.
"Signature Creation Data"	see "Private Key".
"Signature Owner"	Natural person to whom a QEC is issued by ECSP, owns QEC for creating electronic signatures.
"Signature Verification Data"	see "Public Key".
"Signature Verification Tool"	Software or hardware tool that uses the signature verification data to verify an electronic signature.
"Standard (DV) SSL"	The SSL certificate issued and maintained in accordance with DVCP in ETSI EN 319 411-1 standard and "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by "CA/Browser Forum" and verifies domain names.
"Subject"	A person or a server name to appear in the CN field of a certificate.
"Time Stamp Policies"	A document which contains general rules regarding the time stamping and services.
"Time Stamp Practice Statement"	A document which describes in detail how the policies included in the time stamp policy shall be implemented.
"Time Stamp"	An electronic record verified by the ECSP to determine the time when an electronic data has been generated and altered.
"Trust Center"	A unit in ECSP structure; operates registration of certificates from demands of registry authorities; processes application approvals and issues certificates; operates certificate revocation process; creates, manages and publishes certificate records and records of the certificate revocation status.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

According to the Electronic Certificate Service Provider provision, e-tuğra is under obligation of preparing and maintaining necessary documents and records concerning the certification process. Some of these documents and records are published to the public in order to conduct certificate services effectively and to ensure the safety and the continuity of certificate usage.

2.1. Repositories

e-tuğra publishes issued Root and Intermediate CA Certificates, "CRLs", "CPS" and "CP" documents, agreements to be used in ECSP operations, informative documents, relevant audio and visual publications in its Repository. The repository is available for access on the basis of 24 hours every day by certificate owners, third parties and any other interested people. The repository services are available 24/7.

e-tuğra does not employ or use a third party, neither a person nor an enterprise, to publish the relevant documents and records.

2.2. Publication of Certification Information

All the relevant information about the conduct of certification operations is kept public. The institutional procedures about internal operations of the "ECSP" and confidential commercial information are outside this content. The basic information published in repository of e-tuğra is below:

- E-tuğra Root and Intermediate CA Certificates
- E-tuğra Time Stamp and "OCSP" Certificates
- Certificates issued by e-tuğra and those having the written consent of the certificate owner to be published
- E-tuğra's updated "CRL" files
- E-tuğra's "CP" and "CPS" documents
- E-tuğra's Certificate Application Forms, Certificate Agreements
- Corporate Application Agreements
- Documents related to certificate applications
- Informative documents and relevant audio and visual publications

The access to this information referred to in this section is publicly disclosed at e-tuğra's website http://www.e-tugra.com.tr.

The CP and CPS include all the material required by RFC 3647, and are structured in accordance with RFC 3647. CRLs are published in online repositories. The CRLs contain entries for all revoked unexpired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

"e-tuğra" conforms to

- the current version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.0" which is published by CA/Browser Forum at http://www.CAB Forum.org for all SSL certificates,
- the current version of "Guidelines for the Issuance and Management of Extended Validation Certificates v.1.7.8" which is published by CA/Browser Forum at http://www.CAB Forum.org for EV SSL certificates (EVG),
- the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (the "EV Code Signing Guidelines"), published at www.CAB Forum.org,

- the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, published at https://aka.ms/csbr (the "Code Signing Minimum Requirements"),
- CA/Browser Forum Network and Certificate System Security Requirements, and
- other root store policies/programs where eTugra Root Certificates are embedded

In case of any inconsistency between the Requirements and this CPS, the Requirements take precedence over this document.

"e-tuğra" hosts test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate used for SSL. Below are test Web pages for (i) valid, (ii) expired (iii) revoked certificates.

Root for "e-Tugra certification Authority":

i. https://evvalid.e-tugra.com.tr/
ii. https://sslev.e-tugra.com.tr/
iii. https://evrevoked.e-tugra.com.tr/

Root for "E-Tugra Global Root CA RSA v3":

i. https://evvalidrsa.e-tugra.com.tr
ii. https://evexpiredrsa.e-tugra.com.tr
iii. https://evrevokedrsa.e-tugra.com.tr

Root for "E-Tugra Global Root CA ECC v3" :

i. https://evvalidecc.e-tugra.com.tr
ii. https://evexpiredecc.e-tugra.com.tr
iii. https://evrevokedecc.e-tugra.com.tr

2.3. Time or Frequency of Publication

- Any updates in "CP" and "CPS", new versions of the documents are published in the repository along with their old versions as referred in section 9.12 of this "CPS" document.
- E-tuğra Root and Intermediate CA Certificates and certificates to be published by consent of the certificate owner are published on the day of their arrangement.
- Certificate Status Information's are published according to sections 4.9.7 and 4.9.10 of "CPS" document.
- CRLs are published every 6 (six) hours, 4 (four) times a day and with a validity time of 24 (twenty-four) hours.

2.4 Access Controls on Repositories

The Repository is available to the access of all concerned parties in a manner to provide service 24 hours every day. Authorized e-tuğra staff conducts regular controls to ensure the authenticity and the validity of the published information in the repository and it takes all security measures.

3. IDENTIFICATION AND AUTHENTICATION

“e-tuğra” authenticates the identification of new certificate applicants, renewal requests, or electronic address information of webs, e-mail and similar servers for which certificates will be issued and all related contents included on certificates according to legal and technical requirements based on all necessary documents and official sources.

3.1. Naming

3.1.1. Types of Names

Only the types of names supported by X.500 format are used in certificates.

3.1.2. Requirement for Names to be Meaningful

Names in the issued certificates are meaningful and free from ambiguity.

“e-tuğra” Root and Intermediate Certificates contain a fluent subject of CA and commercial title indicating that e-tuğra is an “ECSP”.

In QECs the name fields include names of the QEC owners as they appear in their official documents in the identity verification process and which are verified by e-tuğra.

In SSL and EV SSL Certificates, domain names authenticated by e-tuğra are used.

In Code Signing Certificates (CSC), names of legal entities or real persons which are verified by e-tuğra according to official documents are used.

3.1.3. Anonymity of Certificate Owners, Use of Nicknames, Concealment of the Names of Certificate Owners

e-tuğra does not use anonymous names or nicknames in issued certificates.

According to the Laws and standards, it is not possible to conceal the certificate owner’s name in QECs, Premium (OV) SSL, EV SSL and CSCs. For IDNs, e-tuğra includes the Punycode value of the IDN in the Subject name.

3.1.4. Rules for Interpretation of Different Types of Names

Names on issued certificates are interpreted and prepared according to the X.500 distinguished name form.

3.1.5. Uniqueness of Names

e-tuğra ensures that issued certificates allow unique identification of certificate owners with information contained in distinguished name field. For legislative reasons, distinguished name field may vary according to the type of the certificate.

- E-tuğra ensures that the identity information of different people in QECs is unique in all issued QECs. This uniqueness in QECs is achieved for Turkish nationals by using the Turkish Republic identity number and for residents of other nationalities by using international country code (ISO 3166-1 alpha-3) and passport number. In case any QEC holder has more than one QEC, it is allowed that his/her identity information is the same in QECs.
- In Standard, Premium and EV SSL certificates

- "CN" contains a server name registered in DNS under the name of the subscriber. In Premium wildcard certificates, CN field contains "*.<DNS name>". Wildcards are not issued for EV SSL certificates. CN field can't contain the reserved IP addresses and internal server names. It must be one of the entries in SAN.
- "L" contains the city of incorporation which is indicated in the Turkish Trade Register.
- "C" contains a country code of incorporation that is listed in ISO 3166-1 standard.
- "SAN" contains the "DNS" which is indicated in the "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.

- In Standard (DV) SSL Certificates, distinguishing the certificate owner uniquely is achieved by the field name to which certificate is issued. For these certificates only domain name verification is executed and no kind of organizational verification is executed. Because of the verification level of Standard (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.
- In Premium and EV SSL Certificates, e-tuğra uses a unique name field for legal entities resident in Turkey according to the rules below. In DN field for incorporations:
  - "O" section contains:
    - For Incorporations: The complete name of incorporation as in Turkish Trade Register.
    - For Government Agencies or Public Institutions: Official title in the foundation of the institution which takes place in Organizational Law and related legislations.
    - For Associations, Foundations, Chambers and Unions: Official title in official records.
    - For Business Entities: Official title in up-to-date tax assessment documents.
  - "SERIAL NUMBER" section contains (For Only EV SSL):
    - For Incorporations Companies: contains the unique trade registration number of the center of the incorporation registered in Turkish Trade Register.
    - For Government Agencies or Public Institutions: The unique tax number of certificate owner government institutions.
    - For Associations, Foundations, Chambers and Unions: The unique tax number of certificate owner government institutions.
    - For Business Entities: If applicable (TCKN) Turkish Republic identity number or the unique trade-register number in Turkish Trade Register.

  Note: If the registration number is not available, e-tuğra rejects the request.
  - "OU '' contains the organizational unit or a trademark which is registered in Turkish Standards Institution. Otherwise, it's not used.
  - "GivenName" and "FirstName" if present, natural person Subject's name (For Premium and EV SSL)
- For Uniqueness of Name in Premium (OV) SSL and EV SSL certificates for commercial entities who are not resident in Turkey the same conditions necessary for Turkish residents are required, according to the local regulation, equivalent official vouchers are demanded.

- The relation between the Domain Name and the institution on EV SSL Certificate must be in line with the "Guidelines for Issuance and Management of Extended Validation Certificates" published by "CA/Browser Forum", the procedures according to this guide are applied for EV SSL Certificates.
- To form a distinguished name for "CSC"; "CN" section contains complete name and title of the certificate owner which can be documented officially according to the legislation of the residence, "SERIALNUMBER" section contains the Turkish Republic identity number or Passport number of the certificate owner who is a real person; for legal entities which have their central office in Turkey, unique tax number, for the ones which have their central office outside of Turkey, unique trade register number or code which can be documented according to the legislation of residence are written.

3.1.6. Recognition, Authentication and Role of Trademarks

"e-tuğra" verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification in accordance with section 3.2.2 of the Baseline Requirements.

"e-tuğra" will require a Tradename Registry Letter for national SSL 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.

Certificate owners are responsible for their trademarks to appear and to be used correctly in a certificate application. It is prohibited for certificate owners to use trademarks which violate intellectual property rights of others. If e-tuğra determines any violation regarding the use of trademark names at any certificate application, it holds the right to deny an application or suspend or revoke a certificate.

3.2. Initial Identity Validation

A process is exercised which ensures that the data sources for the validation of certificate content are checked and released in accordance with section 3.2.2.7 of Baseline Requirements.

A procedure is established which ensures that the applicant is contacted via verified communication method defined in 11.5 EVG and can confirm that they are aware of the request and agree to it.

3.2.1. Method to Prove Possession of Private Key

Private Key of "QEC" can only be generated by e-tuğra. In cases where "QEC" and safe electronic signature creation device are handed over to the certificate owner in exchange of his/her signature, it is recognized that the "QEC" owner proves his/her possession of the Private Key.

In other certificates, certificate applicants prove their possession of Private Key by submitting PKCS#10 or equivalent file to e-tuğra. In cases where the Private Key is created in the name of the certificate owner, this condition is not valid.

3.2.2. Authentication of Organization Identity and Domain Control

In cases where a certificate contains the name of an organization (legal entity), the following methods of verification apply according to the type of the certificate. This process of verifying a legal entity is conducted according to e-tuğra procedures which are dependent on the predetermined conditions.

For QEC

In the case of corporate applications and/or in case it is intended to put information on the authorization in QEC on behalf of the relevant legal entity, the identity of the legal entity is verified on the basis of official documents.

For All SSL's

For all SSL certificates, "e-tuğra" validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. The methods are described in Section 3.2.7 "Authentication of Domain Names"

For Standard (DV) SSL

There is no verification of legal identity in Standard (DV) SSL applications.

For Premium (OV) SSL and CSC

The name and the title of the legal entity are verified on the basis of official documents of the country of residence of the applicant according to e-tuğra procedures. The e-mail address submitted by the authorized person who conducts the application process on behalf of the certificate owner should be verified by the authorized person. This verification process is done by sending a distinguished user name and activation code to the e-mail address of the authorized person.

Validation of the Applicant's right to use or control the domain names is performed as in standard SSL.

"e-tuğra" verifies the identity and address of the Applicant using the procedures found in section 3.2.2.1 or section 3.2.3 of the Baseline Requirements. Only applications from entities based on or located in Turkey are accepted for Premium (OV) SSL and CSC.

For EV SSL and EV CSC

Information concerning organization identity related to the issuance of EV SSL/TLS Server Certificates is validated in accordance with the EV Guidelines

In verification of EV SSL applications at least the following conditions must be met:

- "e-tuğra" maintains the blacklist/banned list and checks whether a certificate applicant is enrolled there if yes, application is rejected.
- The name or the title, legal existence and physical existence of the legal entity which will take place in the certificate are verified according to the official documents of the country of residence of the applicant. In addition to this verification, a circular of signature or another valid official document in applicable legislation is required in order to show that the certificate applicant is authorized to represent the legal entity and to sign.
- The operational continuity of the certificate applicant is confirmed by a current official document presented by a public institution or by a legally authorized person to settle the official document.
- The address of the central office of the legal entity of the certificate applicant is verified according to the legal documents of the country of residence along with QGIS and QIIS entries. Moreover, telephone numbers, submitted by the certificate applicant in application forms are cross-checked by legal records. The applicant is called from the verified telephone number in order to confirm the application.
- The e-mail address submitted by the authorized person who conducts the application process on behalf of the certificate applicant should be verified. This verification is achieved by sending a verification email message to the authorized person.

- The domain name which will take place in the certificate must belong to the legal entity or the right and authority to use the domain name must be given to the legal entity by the domain name's registered owner.
- All of the conditions to be met in the verification of the identity of the legal entity in EV SSL certificate applications and the verification process are conducted according to the "Guidelines for Issuance and Management of Extended Validation Certificates" published by "CA/Browser Forum".
- Validation of the Applicant's right to use or control the domain names is performed as in Standard (DV) SSL.
- Any DBA and/or Assumed names will be included in a Certificate must be proofed and verified using a trusted third party or government source.
- Only applications from entities based on or located in Turkey are accepted for EV SSL and EV CSC.
- Legal existence and physical existence of an entity for OV and EV SSL and Code Signing Certificates: Private Organization are verified by a registration form that was taken in the last 6 months from the Chamber of Commerce. Governmental organizations are validated using the KAYSIS system. For other types of organization, a legal letter taken from a related ministry that was produced in the last 6 month is used.
- Verification of Name, Title, and Authority of Contract Signer and Certificate Approver is done with a Notarized Signature Circulars or a Government based documents or Use of a correspondingly secure login method that identified the signer prior to signing.

Others

Country is set 'TR' for QEC. For all other certificate types if Country is used in Subject; it is verified by using the address of the organization who requested the certificate. If organization name is not used in certificate (a) information provided by the Domain Name Registrar (b) the ccTLD of the requested Domain Name; or (b) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address.

In addition to above one of following method being used for validation based on the certificate type, it also ensures the requirements of 11.6 EVG:

1. QIIS
2. QTIS or QGIS
3. Attested verified Letter
4. Independent confirmation from the applicant

Information about QIIS/QTIS/QGSI can be found:

https://mersis.gtb.gov.tr
https://gib.gov.tr/
https://www.kaysis.gov.tr
https://www.ticaretsicil.gov.tr/

These are regularly reviewed and updated according to EVG 11.11.5. All data sources are approved by the "e-tuğra security board".

3.2.3. Authentication of Individual Identity

The identity of the people applying for a certificate is verified by an official and photographed document such as national identity card, passport, driving license which are all given by legal

arrangements. The original official document on which the identity is based during the first application should be presented to e-tuğra or Authorized Registration Units where a photocopy of the official document is taken and it is verified.

When receiving the applications for QECs, and CSC or EV CSC/SSL with the principal individuals (Business entity) are authenticated/validated face to face at the first application.

In QEC applications made by “Corporate Application Owner” identification is conducted according to the “Corporate Application Service Agreement”.

For second and subsequent applications, in cases where it passes more than 6 (six) months after the validity period of the last certificate or there is a change of name or information in the “DN” field, face to face authentication is required again.

In other cases where identification is not necessary, identification can be made via telephone, fax or e-mail according to e-tuğra procedures and instructions.

In cases where a professional title needs to be contained in the certificate, there is a need to submit the official documentation according to the applicable legislation.

3.2.4. Non-verified Subscriber Information

Information of the QEC owner other than the ones in QEC are not supposed to be verified by e-tuğra. The e-mail address in QEC applications takes place in the content of the certificate upon written declaration of the applicant.

For only QEC, other fields such as “L”, “S”, and “O” that may appear in the DN field of a certificate are also accepted as valid upon the declaration of the applicant and they take place in the content of the certificate.

3.2.5. Verification / Proof of Authority

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

For QEC applications requested by "Corporate Applicant", the authority of “Corporate Application Officer” is verified.

For Premium (OV) SSL and CSC, there is a need for an official document to support that the applicant has the authority to act on behalf of the legal entity. The request is verified using a Reliable Method of Communication, in accordance with section 3.2.5 of the Baseline Requirements.

For EV SSL and EV CSC, procedures prepared according to the “Guidelines for Issuance and Management of Extended Validation Certificates” published by “CA/Browser Forum” are applied. The request is verified in accordance with section 11.8.3 of the EV Guidelines.

In the case of organizations, proof of their existence and the right of an authorized signatory to represent the organization is verified and confirmed according to section 3.2.2.

In addition to above applicant info, legal entity info etc. are verified from QIIS, QGIS and QTIS entries.

3.2.6. Interoperability Criteria

“e-tuğra” does not make certification transactions for easing interoperability with another electronic certificate service provider.

3.2.7. Authentication of Domain Names

"e-tuğra" validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements.

- Email to the Domain Contact by sending a Random Value through email to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2;
- Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an e-mail created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the e-mail, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4;
- DNS Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7;
- An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Request Value in the contents of a file (Request Token, Random Value does not appear in the request used to retrieve the file and receipt of a successful HTTP status code response from the request) performed in accordance with BR Section 3.2.2.4.18;
- The other methods are not used in section 3.2.2.4 of the Baseline Requirements.

All of the above methods of validation, may be used for Wildcard Certificate Domain Name ("*.<DNS name>".) validation along with current best practice of consulting a public suffix list.

No certificates are issued for IP Addresses and Internal Names. All names must be authenticated with methods above.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

QECs can be renewed in their validity period, but for QECs for which the validity period has expired it is not possible to re-key. The re-key requests can be done by online application on e-tuğra's web portal, by coming to the central office address or via Registration Authorities. For re-key operations, there is no need to make face to face identification. In suspicious cases e-tuğra may request identification once again. To re-key QECs for which the validity period is not expired, but there is a request to change data in the certificate by the applicant, it is not possible to re-key the certificate, but a new application and verification of identity process is needed, moreover such change must be based on the official documentation.

It's possible to renew or rekey the certificate before the expiration of DV, OV, EV SSL and CSC certificates. Already verified data/information beyond 13 months can't be re-used in both renew and rekey.

If a change in terms and conditions of e-tuğra services has occurred in the period between the initial identity verification and the time of re-key request of the applicant, such change is published on the website of e-tuğra and the applicant is properly informed.

3.3.2. Identification and Authentication for Re-keying After Revocation of Certificate

No re-keying is performed after revocation of certificates and the request for re-keying is treated as a new application and all procedures related to certificate application are conducted.

3.4. Identification and Authentication for Revocation Request

QECs can be revoked by the QEC owner and by corporate application owners or third parties if the QEC owner gives them the permission to do so. In the case the conditions of "CPS" are realized, e-tuğra can also revoke QECs on his own discretion. QECs which contain organization information can be revoked by the person authorized to represent the institution.

QEC revocation and suspension operations can be conducted via e-tuğra's call center, internet site on www.e-tugra.com.tr or by application to RAs. When e-tuğra receives a request for revocation from the concerned parties, it verifies the identity of the person requesting the revocation and his/her authority to make a request for revocation by means of the information received during QEC application and by passwords.

When there is a request for revocation of QEC, the certificate is immediately suspended. With the submission of the written revocation request the certificate is revoked. In the period of suspension, if the certificate owner gives a written notification that the reasons for revocation no longer exist, then the suspension is ended.

Revocation requests for Standard (DV) SSL may be achieved only by the completion of approval operations sent to e-mail addresses taking place in application of certificate. Otherwise authorization of the revocation request is completed by one of the methods of validation of ownership of the domain defined in section 3.2.2.

For Premium (OV) SSL, EV SSL, "CSC" and EV CSC

- Revocation requests are received in writing signed only by the authorized person to act on behalf of the legal entity. The certificate owner or the authorized persons to represent the institution can revoke certificates on e-tuğra's web page by verifying the information given at the application.
- If the applicant is the same real person who made the first certificate application, registered subscriber information is used for identification.
- If the applicant is not the real person making the first application, there is a need for an official document to support that the applicant has the authority to act on behalf of the legal entity.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

“e-tuğra” issues certificates and manages the certificate life-cycle in accordance with the practice statement set forth in this “CPS” document.

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application?

Any real person who does not have any legal obstacles and who fulfills the requirements cited in e-tuğra’s procedures may apply for “QEC” and “CSC”.

Legal entities may apply for “QEC” and “CSC” as corporate applicants on behalf of their employees, customers, members or shareholders.

Any legal entity including public institutions and government agencies may apply for Standard (DV) SSL, Premium (OV) SSL, EV SSL, “CSC” and EV CSC.

"e-tuğra" maintains a Black List in the internal database for previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns.

4.1.2. “Certificate” Application, Enrollment Process and Responsibilities

Certificate Application is formed by two steps such as enrollment and key generation. Enrollment is the verification of certificate application based on documents and the registration in a complete and correct manner. Key generation is the issuance of public and private keys by certificate applicant or by e-tuğra. In case of a key generation by the applicant, the public key should be sent to e-tuğra electronically according to procedures and standards.

QEC Application:

QEC applications can be made by different means of application methods. In order to apply for a certificate, QEC application owners may visit e-tuğra's center or an authorized “RA” which are all listed on e-tuğra’s website. During the QEC application, RA official verifies the identification of the applicant on the basis of an official and photographed identity document such as national identity card, driving license or passport. In the meantime, individual applicants fill out and sign the QEC application form and agreement. The individual applicant delivers to the RA officials a copy of the agreement and the completed application form he/she signs, and other required documents demanded during the application and the ones announced on e-tuğra’s website.

Individual applicants can make a preliminary application by completing the Certificate Application Form available on the web address of e-tuğra. After the completion of the procedures on the web, the individual applicant gets a printout of the contract and of the application form and signs them (if he/she has already a QEC then he/she can sign it with the existing QEC). Then the applicant sends to e-tuğra the application form, the contract signed by the applicant and all required documents of authentication announced on e-tuğra’s web site. If the applicant does not have a QEC, then he/she is required to receive a declaration of signature issued by a notary. After completing these documents, then the applicant sends the notarized declaration of signature, application form, signed QEC user agreement and other requested documents announced on e-tuğra’s website to the relevant e-tuğra unit by registered and reply-paid letter or by courier. The QEC application is completed upon the arrival of the package to e-tuğra.

Public and private keys are generated on the card while QECs are issued on the cards.

Corporate QEC Application:

Corporate application refers to an application made by a legal entity for its employees or customers or members or shareholders. In the case of corporate applications, the applicant appoints a member of its staff who has a valid employment contract with the Corporate Applicant in order to meet the obligations that e-tuğra has assumed according to Corporate Application Agreement Principals on behalf of e-tuğra. The corporate application to e-tuğra can be done through a single application method. The operation of this basic method designated by e-tuğra is as follows:

First of all, a corporate applicant signs the printed Corporate Application Agreement which is published on e-tuğra's website or which is available at any RA office.

The Corporate Applicant appoints simultaneously with the signing of the Corporate Application Agreement, a Corporate Application Official in order to ensure that the obligations of the Corporate Application Agreement are carried out by the Corporate Application Official on its behalf. The corporate applicant completes and signs the Corporate Application Form which is attached to the Corporate Application Agreement. In the Corporate Application Form, The Corporate Applicant specifies the minimum number of Corporate Applications to be made throughout the term of the Corporate Application Agreement, the authorization given to the Corporate Application Official and detailed identification and contact information of that person, moreover any other necessary information about the relevant legal entity. The Corporate Application Officer ensures that the Certificate User Declaration of Commitment, which is an annex to the Corporate Application Agreement also contains the requirements that QEC applications by Corporate Applicant should be documented in writing as per Article 9.2 of the Regulation, is signed by the Certificate Owner, delivering one copy thereof to the Certificate Owner. The Corporate Application Officer concludes the application by delivering to RA official the "ECSP" copies of Certificate User Agreements, Corporate Application Agreement and annexes to it and any other required documents which are requested during the application process and are announced on the e-tuğra's website.

RA verifies the authority of the Corporate Application Official on the basis of the Corporate Application Form and Corporate Application Agreement signed by the Corporate Applicant; it verifies the Identification of the Corporate Application Official on the basis of the photocopies of the national identity card, driving license or passport belonging to him/her and it verifies the authority and identification particulars of the Corporate Applicant on the basis of the circular signature of the Corporate Applicant, Corporate Application Agreement and Certificate User Agreement of Commitment. The demand by Corporate Applicant for assistance by RA or RA official for the registration process to be supervised is met.

SSL Application:

The applications of Standard (DV) SSL, Premium (OV) SSL and EV SSL are all done via e-tuğra's web site. The generation of public and private key is done by the applicant. During the application, the applicant uploads the CSR necessary for the certificate generation to the system. After the completion of the application, a private code is sent to the e-mail address of manager or technical department which takes place in DNS records in order to verify the Domain Name.

Documents published on e-tuğra's web site are delivered or sent to one of e-tuğra's RAs together with the documents showing the authority of the application officials authorized by the application owner. Application owners should agree to a Subscriber Agreement or other applicable terms and conditions during the application process. The application process is ended by inspection and verification of documents according to e-tuğra procedures.

CSC Application:

The application for "CSC" is done via e-tuğra's website. The generation of public and private key is done by the applicant. During the application, the applicant installs the CSR necessary for the

certificate generation to the system. After the completion of the application, a private code is sent to the e-mail address provided at the time of application approval.

Documents published on e-tuğra's website are delivered or sent to one of e-tuğra's RAs. Application owners should agree to a Subscriber Agreement or other applicable terms and conditions during the application process. The application process is ended by inspection and verification of documents according to e-tuğra procedures.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

RA officials perform identification and authentication of QEC application owners, corporate applicants and corporate application officials by means of the methods prescribed by sections 3.2 and 4.1.

During the QEC application the identity of the applicant is verified according to official documents based on legal arrangements.

Applications for certificates of Standard (DV) SSL, Premium (OV) SSL, EV SSL CSC and EV CSC are conducted according to principles and relevant e-tuğra procedures explained in section 3.2.

Re-use of validation information is limited to 398 days for Premium (OV) SSL, EV SSL CSC and EV CSC. Re-use of validation information is not allowed for QEC

"e-tuğra" maintains a database and procedure for identification and requirements additional verification activity for High Risk Certificate Requests.

4.2.2. Approval and Rejection of Certificate Applications

e-tuğra is free to approve or reject the applications made. A certificate application is approved if the following conditions are met:

- One of the application methods which take place in section 4.1.2 should be completed.
- According to the principles explained in section 3.2 and relevant e-tuğra procedures, required forms and documentation should be fully completed.
- Payment of the certificate should be made.

Even if the conditions above are met, occurrence of any of the following conditions leads to the rejection of the application:

- The applicant is not responding satisfactorily or in time to the questions raised for verifying the submitted information and documents.
- In thirty (30) days after the registration of an application of Standard (DV) SSL, Premium (OV) SSL, EV SSL and "CSC", CSR file is not delivered to e-tuğra.
- For a Standard (DV) SSL, Premium (OV) SSL, EV SSL and "CSC" application, there is a strong belief that issuing such certificates may endanger the reputation of e-tuğra.

For a Standard (DV) SSL, Premium (OV) SSL, EV SSL application containing a new gTLD under consideration by ICANN until the gTLD has been approved.

When the application is for Standard (DV) SSL, Premium (OV) SSL, EV SSL, e-tuğra shall examine the authorized CA register, CAA, according to RFC 6844, and if the CAAs are present but do not allow e-tuğra to issue the certificates because it is not registered, e-tuğra will not issue the certificate but will allow applicants to make another request after e-tuğra has resolved the incident.

The Certification Authority CAA identifying domains for CAs within “e-tuğra” operational control are “e-tugra.com”, “etugra.com”, “e-tugra.com.tr”, “etugra.com.tr”.

e-tuğra does not have to show a valid reason when an application is rejected.

4.2.3. Time to Process Certificate Applications

For “QEC”, time to process certificate applications is at most 5 (five) working days after the acceptance of certificate applications. The process of certificate issuance is at most 1 (one) working day after the approval of certificate applications. In obligatory situations, the issuance of QEC may take 45 calendar days according to the smartcard stock.

The applications are processed and issued in 1 (one) day for Standard (DV) SSL, in between 3 (three) and 6 (six) days for Premium (OV) SSL and “CSC”, in between 5 (five) and 12 (twelve) days for EV SSL and EV CSC.

Times given in this section about the application processes are applicable only if certificate applications are accurate and flawless according to the principals and e-tuğra procedures in section 3.2.

4.3. Certificate Issuance

4.3.1. Action of “ECSP” During Certificate Issuance

After the approval of the application following the completion of the application processes defined in section 4.2.2, accepted certificates are issued in e-tuğra’s Trust Center.

After the application processes are completed and the applications are accepted, the certificates are issued by passing a two-tier approval process by “e-tuğra’s Secure Staff” within the Trust Center.

For QEC, public and private keys are issued in accordance with the algorithms and parameters indicated at the Communiqué in the secure electronic signature creation device belonging to the certificate owner. QEC connected certificate with a public key belonging to the certificate owner is issued in line with the information received from the “QEC” application owner.

Certificates for Standard (DV) SSL, Premium (OV) SSL and especially EV SSL are issued according to the rules defined in 11.3, 14.1.3 & 16 EVG explicitly 4 eye principles in the presence of trusted staff authenticated via multifactor by the use of the “CSR” sent by the applicant and then the issued certificate packaged together with the intermediate and root certificates and it is sent back to the applicant’s email address verifying domain name.

“CSC” or EV CSC is issued by using the “CSR” sent by the applicant and then the issued certificate packaged together with the intermediate and root certificates is sent back to the e-mail address declared and verified during the application process.

Before issuing SSL/TLS certificates pre-issuance linting (custom developed and zlint) being used and “e-tuğra” uses CT according to RFC 6962 and ensures browser requirements of publication in two or more CT databases. “e-tuğra” CA handles the revocation of pre-certificate meeting the Mozilla recommended practices.

“e-tuğra” uses current system time for notBefore and it is sync with NTP Server. It's not possible to backdate current time as the CA clock is sync with NTP server.

Certificate issuance by the Root CA is not allowed for subscriber certificates.

4.3.2. Notification to Certificate Owner about the Issuance of Certificate

After the certificate is issued, the certificate owner is informed by e-mail or SMS message about the issuance of the certificate.

4.4. Certificate Acceptance

4.4.1. Operations Deemed Acceptance of Certificate

The act of receiving the certificate issued by e-tuğra is deemed as the acceptance of the certificate. For all kinds of certificates, certificate owners are under obligation to review and verify the accuracy of the data in the certificate before installing or using it and to notify e-tuğra and request revocation of the certificate if it includes data that is inaccurate or inconsistent with the information given during the application. If the so-called inconsistency of data is caused by e-tuğra, then the issuance of the new certificate is done by the forms filled out by the applicant.

For QECs, in case the equipment in the package of QEC sent to the certificate owner is incomplete or defective, then the QEC owner should notify e-tuğra in 7 (seven) working days.

If the QEC package is not received by courier or from RA's offices within 1 (one) month after its issuance, then the certificate is taken into account as not accepted, it is revoked and no refund is paid.

In cases where the delivery of certificates for Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC is made to certificate owners and there isn't any disapproval within 7 (seven) days, then the certificate is deemed accepted.

4.4.2. Publication of Certificates by "ECSP"

QECs can be published only by written consent of the certificate owner in the web or directory servers open to the public.

4.4.3. Notification of Certificate Issuance to Other Concerned Parties

Not applicable.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Certificate Owners are under obligation to use their certificates and their private key in accordance with the obligations cited in relevant Law, Regulation, Communiqué, other regulatory actions, the "CP" and "CPS" documents and the related certificate user agreements. Moreover, if there are limitations regarding the use and the physical content of the certificates, then the certificate should be used within these limitations.

Certificate owner is under obligation to ensure confidentiality and the security of the private key and of the activation data and to prevent any unauthorized use thereof. Certificate owners must immediately inform e-tuğra in case of any suspicion over the confidentiality or security loss, theft or security compromise of the private key, of the signature creation device or of the activation data.

For QEC, the certificate owner should receive in person the electronic signature creation device issued to his name and activation code belonging to this device, if it exists. The QEC owner should not allow other people to use his mobile phone or e-mail address for those circumstances when the activation code is used.

4.5.2. Relying Party Public Key and Certificate Usage

Third parties who will conduct business and transactions relying on the certificates of “e-tuğra” must first check the certificate. Certificate owners are under obligation to use their certificates in accordance with the obligations cited in relevant Law, Regulation, Communiqué, other regulatory actions, the “CP” and “CPS” documents.

If there is any doubt about certificate validity control to be done under secure and appropriate conditions, then third parties take necessary precautions. Before relying on a certificate, third parties should check:

- Whether the certificate is used in accordance with its usage purpose;
- 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 certificate conforms key usage field value,
- Whether the certificate is issued by e-tuğra;
- Whether the certificate, the root and intermediate certificates on which the certificate is based on are valid. (For this issue “e-tuğra” provides uninterrupted CRL and OCSP services).

During these operations third parties are under obligation to use secure software and hardware defined by the legislation and standards.

In cases where the checking and verifying procedures fail, third parties should not rely on these certificates.

“e-tuğra” cannot be held responsible for third parties not fulfilling the conditions about the use of public key and certificate.

4.6. Certificate Renewal

Certificate renewal operations are made only for QECs which are subject to renewal processes explained below. Certificate renewal for QEC is the extension of QEC’s validity term without making any changes in public key. In order for a certificate to be renewed, the private key of the certificate should not have been compromised. For QECs of which validity term is expired certificate renewal cannot be made. For the security of the keys, the validity term of a certificate having the same data cannot be longer than 3 (three) years.

4.6.1. Circumstances for Certificate Renewal

Certificates can be renewed upon the request of the certificate owner only before the expiry date of QEC’s validity term and with the condition that there isn’t any change in the content of the certificate. An expired certificate can also be renewed provided that the renewal request is done within the validity term of the certificate.

4.6.2. Who May Request Renewal?

The certificate owner or a person authorized to represent the certificate owner may request certificate renewal.

4.6.3. Processing Certificate Renewal Requests

Certificate renewal is only made for QECs. Renewal requests can be made via e-tuğra website or RAs. In case the renewal request is made on the web, the application form for certificate renewal is completed and signed by the secure electronic signature of the certificate owner requesting the certificate renewal. E-tuğra by verifying the secure electronic signature of the certificate owner requesting certificate renewal makes the identification of the QEC owner. In certificate renewal requests made to RAs, the RA official makes the identification on the basis of official ID documents such as national identity card, driving license and passports. After the identification is completed, the new QEC is issued upon the fulfillment of necessary verifying procedures and payment controls.

4.6.4. Notification of Renewed Certificate Issuance to Subscriber

Principles of section 4.3.2 apply.

4.6.5. Operations Deemed Acceptance of QEC Renewal

The installation of the new certificate by certificate owner which is the final step in QEC renewal procedures is deemed acceptance of the certificate renewal. Principles of section 4.4.1 apply.

4.6.6. Publication of Renewed Certificate by "ECSP"

Principles of section 4.4.2 apply.

4.6.7. Notification of Certificate Issuance to Other Participants

Not applicable.

4.7. Certificate Re-key

"e-tuğra" performs re-keying operations only for QEC in special conditions mentioned below. Except these conditions re-key is not applicable. Renewal operations are just conducted as part of the certificate renewal. In cases where there is a need for re-keying, QEC is revoked and a new QEC is issued by initiating the QEC application process.

4.7.1. Circumstances Requiring Re-keying of Certificates

In cases where a QEC is erased from the smart card, or the card is lost, or the card doesn't function properly, in the first 1 (one) month of the validity term, a new certificate is issued just once with re-key without any new documentation for verification but with the condition that the data submitted at the certificate application remains unchanged.

4.7.2. Who May Request Certificate Re-keying?

For QEC, a real person who is the owner of the certificate may request certificate re-keying.

4.7.3. Processing Certificate Re-keying Requests

In case of any suspicion about the conditions mentioned in section 4.7.1, relevant information and supporting documents are required again.

4.7.4. Notification of New Certificate Issuance to Certificate Owner

Principles of section 4.3.2 apply.

4.7.5. Operations Deemed Acceptance of Re-keying of Certificate

Principles of section 4.4.1 apply.

4.7.6. " Publication of the Re-keyed Certificate by “ECSP”

Principles of section 4.4.2 apply.

4.7.7. Notification of Certificate Issuance by “ECSP” to Other Concerned Parties

Not applicable.

4.8. Certificate Modification

4.8.1. Circumstances Requiring Certificate Modification

Modifications to the content of a certificate can be made only when the certificate is revoked or there is a change in the content of the certificate by the issuance of a new certificate. Such a modification requires a new certificate application process to be initiated.

4.8.2. Who May Request Certificate Modification?

Principles of section 4.1.1 apply.

4.8.3. Process of Certificate Modification Requests

Principles of section 3.2 apply.

4.8.4. Notification of New Certificate Issuance to Certificate Owner

Principles of section 4.3.2 apply.

4.8.5. Operations Deemed Acceptance of Modified Certificate

Principles of section 4.4.1 apply.

4.8.6. Publication of the Modified Certificate by “ECSP”

Principles of section 4.4.2 apply.

4.8.7. Notification of Certificate Issuance by “ECSP” to Other Entities

Not applicable.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances Requiring Certificate Revocation

e-tuğra will revoke a certificate within 24 hours after acknowledge and one or more of the following occurs:

- Request by the certificate owner or by the person authorized to represent in writing which can be made via e-tuğra's official website, call center over phone, by sending e-mail and signing by secure electronic signature or in a written way;
- e-tuğra obtains reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
- e-tuğra is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
- The certificate owner/authorized person/subscriber notifies e-tuğra that the original Certificate request was not authorized and does not retroactively grant authorization;
- e-tuğra obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

e-tuğra may revoke a certificate within 24 hours and will revoke certificate within 5 days after acknowledge and one or more of the following occurs:

- The certificate no longer complies with requirements defined in section 6.1.5 and 6.1.6 of CA/B baseline requirements or any section of the Mozilla root store policy;
- It is discovered that the certificate is being used to enable criminal activities such as phishing attacks, fraud or the distribution of malware or mis-used;
- It is evident that the certificate has been used in contradiction to the provisions of the "CP" and "CPS" guide documents and Letter of Commitment and Certificate User Agreement;
- e-tuğra confirms any evidences or circumstances showing that use of a FDQN, IP address or email in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- It is understood that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- There is a change of the information in the content of the certificate or about the certificate owner;
- As a result of "e-tuğra"s sole discretion, during the administration of certificate, detecting non-compliance on the principles of "CPS" guidebooks and on the policies of related "CP". Also, the certificate is not issued in CA/B requirements or related browser policy;
- e-tuğra identifies that the information in certificate is false / incorrect or inaccurate; e-tuğra may be of the opinion that this circumstance took place relying on plausible evidence; moreover, the same circumstance may take place by the notification of the certificate owner or the person authorized to represent;

- The right of e-tuğra to issue certificates under CA/B forum requirements / QEC based on Law has expired or revoked or terminated, unless e-tuğra has made arrangements to continue maintaining the CRL/OCSP repository;
- Revocation is required by e-tuğra CP and/or CPS;
- e-tuğra confirms a demonstrated or proven method that exposes the certificate owner Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed OR Any of the algorithms, or associated parameters or key length, used when creating certificates are compromised or become insufficient for its remaining intended usage;
- The private key has been lost, stolen, disclosed or there is a revelation of a risk of access or use by a third party;
- The certificate owner has lost his/her control over the private key due to the revelation of the activation code or a similar reason;
- The software or hardware in which the private key is located has been lost, broken or become insecure.

In Addition, for QEC certificate revocation one or more of the following can occur:

- After the issuance of the certificate, if the e-signature package that is to be delivered through RA is not received by the certificate owner within 1 (one) month, if the e-signature package that is to be delivered by courier is not taken by the certificate owner within 1 (one) month.
- The right of e-tuğra to issue certificates for QEC based on Law has expired or terminated.
- Termination of the legal relationship which serves as a basis for Corporate Application between the Corporate Application Owner and the Certificate Owner.
- e-tuğra or the Corporate Application Owner suffers damages as a result of an intentional action performed by the certificate user through the use of QEC.
- Establishment by e-tuğra or Corporate Application Owner that QEC is used by the certificate owner unlawfully or for purposes against the areas of use or physical scope contained by QEC.
- There is a change of the information in the content of the certificate or about the certificate owner.
- It is learned that the certificate owner's legal capacity is restricted, or the certificate owner is bankrupt or lost, or died.

e-tuğra will revoke a Subordinate CA Certificate within seven (7) days after acknowledge and one or more of the following occurs:

- e-tuğra obtains request revocation from Subordinate CA in writing;
- The Subordinate CA notifies e-tuğra that the original Certificate request was not authorized and does not retroactively grant authorization;
- e-tuğra obtains evidence that the Subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or doesn't comply with requirements defined in section 6.1.5 & 6.1.6 of the CA/B forum requirements & any section of the Mozilla Root Store policy;
- e-tuğra obtains evidence that the certificate was misused,
- e-tuğra is made aware that the certificate was not issued in accordance with the BR or the applicable Certificate Policy or Certification Practice Statement documents,
- e-tuğra determines that any of the information appearing in the certificate is inaccurate or misleading,

- e-tuğra or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate,
- e-tuğra or Subordinate CA's right to issue certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository,
- Revocation is required by e-tuğra'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?

Certificate revocation requests can be done by the following people:

- Certificate owner for QECs, in case there is institutional information in QEC the authorized people to represent legal entity, corporate application owners in case they have such authorization,
- Certificate owner for "CSC", in case there is institutional information in "CSC" the authorized people of the legal entity,
- Domain name owner or application owner for Standard (DV) SSL,
- The authorized person to represent the certificate owner legal entity for Premium (OV) SSL, EV SSL and EV CSC,
- Public institutions and court authorities which have such authorization,
- E-tuğra staff in necessary circumstances.

Third Parties who are identifying to be a problem with a certificate such as related to fraud, misuse, or compromise.

4.9.3. Procedures for Revocation Request

"e-tuğra" gives certificate revocation service continuously on a 24/7 basis via e-tuğra's support website or email or call center.

For all types of SSL ve CSC certificates, revocation request by certificate owner is taken by call center, "e-tuğra" support web sites, email or with declarative statements. Third Parties may request a revocation via email, or "e-tuğra" support web site providing the reason for revocation.

Public revocation contact information is given section 1.5.2.

Revocation requests for QECs shall be received via different ways such as e-tuğra's support website, call center, email and declarative statements written by the certificate owner (signed papers sent by fax or mail to e-tuğra or RAs). On each communication method, a declarative statement is requested and the certificate owner is verified.

- If the certificate owner requests revocation via telephone, then he/she reaches the authorized operators through the telephone number announced for the call center. The certificate owner completes the authentication steps by entering Turkish Republic national identity number and confirmation number sent to him/her and all other information requested through the registered mobile phone or e-mail. Then the certificate owner completes the certificate suspension or revocation operation.
- For QECs, certificate owner or the authorized person may also inform e-tuğra by a hand written and signed revocation request. When the original copy or copy of the request reaches e-tuğra,

it will communicate with the certificate owner via using contact information on the system and after passing the identity validation process the certificate is revoked. If the communication is not established with the certificate owner, the certificate is suspended until contact with the owner.

- For QECs, the corporate application owner or the authorized person to represent the corporation may inform e-tuğra only by a written and signed certificate revocation request. When the original copy of the request reaches e-tuğra, the certificate is revoked by verifying the signature on the written request. If the certificate revocation request is sent by fax or by e-mail in a scanned form, then the certificate is suspended until the original copy arrives. After this operation, the revocation status is notified to the certificate and corporate application owner.
- If there exists a corporate expression in the certificate, revocation requests for QECs may be received from certificate owners as well as from the authorized people representing the related corporation with approved revocation applications. After the verification of the written revocation request by authorized people, the revocation is completed. After this operation, the revocation status is notified to the certificate owner.

Revocation requests for Standard (DV) SSL may be achieved by the completion of approval operations sent to email addresses taking place in application of certificate. If this method is not applicable, it can be confirmed with the e-mail addresses in the DNS records of the domain name or FTP or CNAME options. For Premium (OV) SSL, EV SSL, “CSC'' and EV CSC,

- Revocation requests are received in writing signed only by the authorized person to act on behalf of the legal entity. After the verification of the written revocation request, the revocation is completed. After this operation, the revocation status is notified to the authorized person.
- If the applicant is the same real person who made the first certificate application, the revocation process is completed by using the confirmation code sent to him via his mobile phone or e-mail registered in the “e-tuğra”.
- If the applicant is not the real person making the first application, “e-tuğra” requests and verifies the authorization documents of the applicant for the organization inside the certificate subject.

If the application is received by email, “e-tuğra” support website or call center, a written request signed by the authorized person is received. Third Parties may report a problem in a certificate like related to fraud, misuse, or compromise via the e-mail, support website or Call Center published for the purpose of revocation.

In cases where there is a security problem on the side of e-tuğra, or a notice is received regarding the existing certificates, or a mistake is found in the certificate issuance process, then e-tuğra may initiate certificate revocation. For this kind of certificate revocations, the outcome is notified to related certificate users by email. In necessary cases, new certificate issuance operations are started after the revocation without asking for a fee.

A revoked certificate cannot become reusable.

In cases where root and intermediate certificates are revoked, the status is notified in electronic media to all related parties immediately in the shortest possible time. End user certificates that have the signature of the revoked root and intermediate certificates are also revoked and users are notified by email.

4.9.4. Certificate Revocation Request Grace Period

In cases where technical and commercial opportunities are available, the certificate revocation request is processed within the shortest period of time by e-tuğra. After the approval of the certificate revocation request, such certificate is included in the first "CRL" to be published and this period cannot be longer than 24 hours.

Revocation lists are published at http://crl.e-tugra.com, http://crl1.e-tugra.com addresses for each certificate authority.

4.9.5. Processing Time for Certificate Revocation Request

"e-tuğra" concludes within the shortest period of time all certification requests sent via web 7 days and 24 hours as long as the request is adequate and the technical and commercial opportunities allow.

For QEC revocation requests received via written statement are taken into process immediately within the working hours and the revocation process is completed in 24 hours.

For SSL and CSC, revocation requests received via written statement or email or phone or via online section of "e-tuğra" web are taken into process immediately. "e-tuğra" investigates the facts and circumstances involved with the request and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After the revocation request is approved the certificate takes place in the first "CRL" to be published.

4.9.6. Checking Liability of Third Parties about Revocation

Third parties are under obligation to check the present validity status of a certificate prior to proceeding with any business or transaction based on a secure electronic signature. Third parties must check certificate validity status by means of "CRL" and "OCSP". For the purpose of meeting their control obligations specified by "CP", "CPS" and the Regulation, e-tuğra recommends that third parties use secure electronic signature verification tools which are adequate to CWA 14171 Standards.

4.9.7. Frequency of Publication of Certificate Revocation List (CRL)

"CRLs" for QECs are published once at least every 24 hours, in order to be valid for 24 hours; "CRLs" for Standard (DV) SSL, Premium (OV) SSL, EV SSL and "CSCs" are published at least once every 24 hours in order to be valid for 1 (one) week at the most; "CRLs" for intermediate certificates are published when one of immediate certificate is revoked, otherwise once every 6 months in order to be valid for 6 months. E-tuğra provides "CRL" service 24 hours 7 days.

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.

4.9.8. Timing for Publication of "CRLs"

CRLs are published immediately after they are issued, within 10 minutes at the most at the addresses http://crl.e-tugra.com and http://crl1.e-tugra.com.

4.9.9. Accessibility to Online Revocation Control

"e-tuğra" provides uninterrupted "OCSP" service ensuring real time certificate revocation status control. "OCSP" service is based on the installation of appropriate software by users to access e-tuğra's

"OCSP" provider, transmission of status control requests and provider sending replies to requests online. Certificate owners and third parties can use the secure electronic signature verification device to make use of "OCSP" service.

Within the scope of "e-tuğra" 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 "e-tuğra" is signed using an OCSP responder certificate that is issued by the root or sub root certificate that issued the queried certificate.

"e-tuğra" 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.

4.9.10. Online Revocation Checking Requirements

It is recommended that when inquiring about the status of certificates, third parties should prefer "OCSP".

Any change on a subscriber and all other type certificate status are published to the OCSP servers automatically.

"e-tuğra" supports an OCSP capability using the GET method for all Certificates. The servers will not respond with a "good" status for a certificate that has not been issued.

4.9.11. Other Forms of Revocation Advertisements Available

"e-tuğra" does not use any other method than "OCSP" and "CRL" for publishing revocation status.

4.9.12. Special Requirements Regarding Key Compromise

For All SSL and CSC Certificates, If "e-tuğra" discovers or suspects that a Private Key has been compromised, it will make commercially reasonable efforts to notify the Trusting Parties. "e-tuğra" will use "key compromise" in a CRL upon discovery of such reason or as required by an applicable CP.

Reports to "e-tuğra" for Key Comprise include:

- The private key itself.
- A valid email address so that confirmation of your problem report and associated certificate revocations will be sent.

"e-tuğra" provides specific instructions and support for Key compromise on the following website: https://helpdesk.e-tugra.com.tr/submit_ticket and other resources as indicated in section 1.5.2 of this CPS. Once you submit the ticket on this URL, one can select the right purpose i.e. Certificate Revocation and write more details about the key compromise in the Message section. For other methods pointed in section 1.5.2, more details about the key compromise can be provided.

"e-tuğra" may revoke root and intermediate certificates in case there is a suspicion about the confidentiality and security compromise of the private keys. If root and intermediate certificates are revoked, all certificates which are issued by these certificates are also revoked. The status of revocation of root and intermediate certificates and of all other certificates issued by them is notified to certificate owners and third parties.

For all certificate revocation operations originating from "e-tuğra", new certificate issuance operations are started immediately by "e-tuğra".

In case there is a security problem regarding end user certificates, then such certificates are revoked and certificate owners are informed.

4.9.13. Conditions for Certificate Suspension

Suspension of QEC means that the QEC in question has been rendered ineffective for a temporary period of time. The difference between the suspension of a certificate and the revocation of a certificate is that it is not possible to activate the revoked QEC effectively again, the suspended QEC can be rendered effective again upon the removal of the suspension status. “e-tuğra” suspends any QEC in response to suspension requests made by QEC owners and authorized people.

In cases where the source of a certificate revocation request cannot be determined, e-tuğra suspends the relevant certificate until the verification process is completed.

Suspension operations are not applied for other kinds of certificates.

4.9.14. Who Can Apply for Suspension?

For QEC, principles in section 4.9.2 apply. Suspension operations are not applied for other types of certificates.

4.9.15. Process of Certificate Suspension Requests

For QEC, principles in section 4.9.3 apply.

In cases where a security compromise occurs at e-tuğra, or a notice is received regarding the existing certificates, e-tuğra may suspend relevant certificates until the revocation requirement becomes definite. At this kind of certificate suspension operations, the outcome is announced to relevant certificate owners and users by email.

Suspension operations are not applied for other types of certificates. Suspension operations are not applied for root and intermediate certificates.

4.9.16. Limits on Suspension Period

The operation for suspension for “QEC” can continue until the end of the certificate validity term.

The suspended certificates in cases where the source of a QEC revocation request cannot be verified remain in suspension status until the verification process is completed or time limit is over. QECs which are suspended because the certificate owner is not sure whether any circumstance that requires revocation exists are revoked when the revocation requirement is approved by the QEC owner. QECs which are still at the suspension status at the end of this security period are automatically revoked. If it is understood during the period of suspension that there is no need for revocation, then the certificate may be taken out of suspension and the certificate may be valid again.

Suspension operations are not applied for other types of certificates.

4.10. Certificate Status Services

Certificate status service is given by 2 (two) different methods: Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). Revocation status information includes information on the status of certificates at least until the certificate expires.

4.10.1. Operational Features

Certificate status checks can be done by “CRLs” and “OCSP”. E-tuğra provides CRL and OCSP services 24 hours 7 days in an uninterrupted way from the following web addresses:

- http://crl.e-tugra.com,
- http://crl1-etugra.com
- http://ocsp.e-tugra.com,
- http://ocspvs.e-tugra.com,
- http://ocspvn.e-tugra.com

"e-tuğra" publishes QECs in a publicly accessible directory subject to the written consent of the QEC owner.

4.10.2. Service Accessibility/Availability

"e-tuğra" provides "CRL" and "OCSP" services without interruption 24/7. These services are not unavailable for no longer than 1 hour.

"CRL" service is also offered from a different physical place which is a second server.

In order to prevent "OCSP" services from being interrupted, certificate services offered at e-tuğra's center are always sustained by a Disaster Rescue Center that has sufficient level of infrastructure for availability, accessibility and start over purposes. In cases where a situation beyond the control of e-tuğra arises that leads to interruption of services, then e-tuğra's Disaster Rescue Center takes over the management of certification services.

4.10.3. Optional Features

Not applicable.

4.11. End of Subscription

Certificate ownership ends upon the expiry of the validity of a certificate or the revocation of a certificate.

4.12. Key Escrow and Recovery

E-tuğra does not back up or does not store private keys of certificate owners, neither it regenerates, nor it provides data recovery services.

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 describes the core physical and operational controls and procedures that “e-tuğra” carry out as an “ECSP” when delivering certificate services. “e-tuğra” performs its operations regarding network security according to Communication and Operation Management Procedure, meeting the requirements of ETSI EN 319 411-1, Baseline Requirements Network and Certificate System Security documents.

5.1. Physical Controls

5.1.1. Site Location and Construction

“e-tuğra” carries out all core “ECSP” operations, including certificate life cycle management and key management, within a physically protected “Trust Center” that has various security areas designed to stop, prevent and detect covert or open attacks.

5.1.2. Physical Access

Access to “e-tuğra”s “Trust Center” requires getting past a security system that is protected by multiple security levels. There are two types of security levels: access to the external site and access to the “Trust Center”. Access to the “Trust Center” is only possible after accessing the external site. Methods such as personal access cards for staff, Identification checks and registration for visitors are employed for access to the external site. Access to the “Trust Center”, where certificate life cycle management and key management operations are performed, require further security clearance. The “Trust Center” can only be accessed by “trusted staff” using biometric identification methods and all entries and exits are logged. The “Trust Center” is monitored 24/7 by security cameras and the camera recordings are maintained.

Visitors who are present in the building for maintenance and support activities, meetings and similar reasons are not left alone and oversighted by authorized “e-tuğra” personnel.

5.1.3. Power and Air Conditions

Uninterrupted power supplies and generators are installed to ensure the uninterrupted operation of the hardware used at the “Trust Center” and for “e-tuğra”s core “ECSP” operations. In addition, heating/ventilation/air conditioning systems are also in place to monitor the ambient temperature and relative humidity.

5.1.4. Anti-flood Protection

“e-tuğra”s “Trust Center” is built on the top of the building for protection against flooding and is equipped with appropriate insulation systems. Areas and sections where critical hardware and equipment are located are separated from the plumbing and sewerage systems. In case of any flooding, the area is equipped with sensitive water sensors that detect 1 mm of water on the floor level and set the alarm on.

5.1.5. Fire Prevention and Protection

“e-tuğra” has taken all necessary measures to prevent and extinguish fires as well as flames or smoke that can lead to damage. The “Trust Center” is reinforced with additional fire prevention and extinguishing systems. In addition, the whole building is equipped with fire extinguishers and all staff is continuously trained to fight fires.

5.1.6. Data Media Storage Environments

Software and data used in operations as well as all media containing audit, archive or back-up data are stored in the "Trust Center" or in secure environments, accessible by authorized persons only, that are designed to protect the media against any accidents and damage (e.g. water, fire and electromagnetic interferences) and have proper physical access controls in place.

5.1.7. Waste Control

All documents used throughout the certificate life cycle management and in other "e-tuğra" "ECSP" operations and have become ineffective and/or unnecessary are destroyed according to the applicable procedures. Any secure electronic signature creation devices and other relevant cryptographic hardware are physically destroyed or reset according to the manufacturer's instructions. All the other wastes are taken out of the building according to normal waste disposal procedures.

5.1.8. Off-site Back-up

To ensure the business continuity of certification management services, "e-tuğra" maintains back-ups of electronic records on-site at the "Trust Center" and off-site, according to the "Business Continuity Plan" and "Disaster Recovery Plan", as a measure against any potential technical breakdowns and/or disasters.

5.2. Procedural Controls

5.2.1. Trusted Roles

Management controls for certificate life cycle and electronic certificate services, key management controls, and "e-tuğra" management systems and repository controls are conducted by "trusted staff" that have access and control authorization. "Trusted Staff" members are selected among individuals who have adequate knowledge and experience in "PKI" technology, data security and risk management. The following "e-tuğra" "trusted staff" definitions shall apply:

- **Senior Managers:** are responsible for the technical and administrative implementation of "e-tuğra" certificate services.
- **Security Manager**: is "trusted staff" assigned with the duty, power and responsibility to identify, implement, and approve all policies and principles related to the information security management system.
- **Trust Center Manager:** is "trusted staff" responsible for the entire technical management of the security applications.
- **Certificate Operators:** are "trusted staff" assigned and authorized to perform operational processes such as application document controls, certificate registration, certificate issuance, revocation and suspension.
- **Registration Authority (RA) Operators:** are "trusted staff" assigned and authorized to perform operational processes such as application document controls, certificate registration, and revocation and suspension requests.
- **System Administrator (Network and System Administrator):** are "trusted staff" assigned and authorized to install, configure and maintain "e-tuğra"s "ECSP" secure systems to deliver certificate services and management. In addition, they are assigned and authorized to use "e-tuğra"s "ECSP" secure systems on a daily basis and perform system back-up and recovery.

- **System Auditors:** are “trusted staff” that are assigned and authorized to access “e-tuğra”s “ECSP” secure system audit records and archives and ensure their continuity.

“Trusted staff” are selected and assigned among individuals that meet the criteria in Section 5.3 by a manager fully authorized in terms of security.

5.2.2. Number of Staff Needed for each Role

All “e-tuğra”s critical operational procedures are performed by at least two “trusted staff” in accordance with the relevant instructions. Critical operational procedures are high-security applications that require the use of cryptographic devices.

All issuance, renewal and revocation operations relating to “e-tuğra”s "ECSP" root and intermediate certificates require at least two manager-level “trusted staff” that are duly qualified and authorized.

5.2.3. Identification and Authentication for Each Role

Individuals assigned as “trusted staff” are entered into the security system with their identification and biological data and designated rights. An authority checks and identification is performed before 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

Certificate life cycle management operations, “ECSP” key management operations and relevant controls are performed by at least two trusted staffs who have different responsibilities. The principle of separating responsibilities prevents a single person from performing the whole or major part of an operation. Each operation is logged to include the date, role and name of the staff performing the operation.

When assigning responsibilities and roles the management team follows the below principles:

- Actions that require confidentiality such as purchase orders and confirmation of the delivery of goods are separated to prevent fraud;
- In case of any potential confidentiality breach, the number of staff responsible for the action is increased;
- The responsibility to manage system access controls is separated from all other responsibilities that may compromise security controls;
- All creation, modification and removal requests regarding user access rights are processed upon the approval of the Trust Center Manager and Security Manager. Such requests and the relevant actions are logged. The documents are kept for not less than one year for possible future controls;
- The System Administrator reviews system access rights at regular intervals and lifts such rights when not needed. Responsibilities are assigned to check and manage shared passwords;
- Additional controls apply for high-risk tasks;
- User Identifications and passwords are distributed to system users in a secure manner.

With the exception of the below, staff assigned to trusted roles cannot be assigned to a second trusted role.

- The Security Manager can also be the Trust Center Manager.

- Senior managers may assume a second trusted role.

5.3. Personnel Controls

5.3.1. Qualification, Experience and Clearance Requirements

“e-tuğra”s recruitment policy is built on its “ECSP” requirements. The recruitment policy is comprised of two sections: the recruitment of general staff and “trusted staff”. “e-tuğra”s general staff consists of employees assigned to marketing, organizational and administrative roles, without any involvement in the “Trust Center” operations. All recruitments and assignments require a security clearance.

Individuals demonstrating the required qualifications, education and confidentiality are recruited as general “e-tuğra” staff by senior managers.

Trusted staffs are recruited at the discretion of senior managers after documenting that they possess the required professional knowledge, qualifications and experience to perform their duties in a satisfactory and proper manner. Background checks for “trusted staff” are carried out at least every five years.

Recruited staff must not have been convicted of the following crimes (excluding negligent crimes): heavy imprisonment or imprisonment of more than six (6) months, even if pardoned; infamous crimes such as basic and complex embezzlement, extortion, bribery, theft, fraud, counterfeiting, breach of trust, and fraudulent bankruptcy; smuggling crimes except for the use and consumption of smuggled goods; bid rigging in public tenders and procurements; money laundering; disclosure of state secrets; tax evasion or involvement in tax evasion; or, cyber-crimes.

5.3.2. Professional Background Checks

A series of security and background checks are performed before “e-tuğra” general staff and trusted staffs are recruited. These include the primary source verification of references, previous employment, education, qualifications, and criminal record as well as an assessment of technical and administrative suitability.

5.3.3. Training Requirements

Prior to assignment, “e-tuğra” staff receive legal and technical training in “ECSP” services, certificate life cycle management services, professional responsibilities, core public key infrastructure framework, Registration Authority and “Trust Center” operations, “e-tuğra'' security procedures, and certificate policies. “e-tuğra”s training are periodically revised and updated as needed.

"e-tuğra" maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges.

Registration officers are trained and evaluated enough for the EV certificates validation criteria defined in EVG 14.1.2.

5.3.4. Training Frequency and Conditions

In addition to the initial training, “e-tuğra” staff receive updated training at regular intervals. The frequency and content of the training are subject to change in line with the organization’s performance analyses. Training may be delivered in the case of any change or update in “e-tuğra”s operations, software and hardware or as needed.

5.3.5. Job Rotation Frequency and Sequence

"e-tuğra"s management may subject its staff to rotation, as deemed necessary and appropriate, on the basis of their knowledge, skills and experience.

5.3.6 Sanctions for Unauthorised Actions

"e-tuğra" shall take disciplinary action and exercise the penal clauses laid down in the non-disclosure agreement in the event that the security and operational policies are breached. If "e-tuğra" or its customers incur any damage due to such breach "e-tuğra" may seek indemnification from the individual responsible for the breach.

Legal action shall be taken in the event that unauthorized actions or procedural breaches are included in the crimes defined in the Electronic Signature Law, the Turkish Penal Code (Law) or other relevant laws.

5.3.7. Independent Contractor Requirements

"e-tuğra" may enter into agreements with independent contractors to perform its "ECSP" operations. Such service agreements shall be compatible with "e-tuğra"s security and operational procedures.

Contractor personnel employed for "e-tuğra" operations are subject to the same process, procedures, assessment, security control, skills and training as permanent CA personnel.

5.3.8. Documents Provided to Staff

"e-tuğra" provides all staff with "CPS" and "CP" documents, procedures related to certificate services, security procedures and instructions as well as specific software and hardware manuals related to their respective roles.

Delegated Third Party's personnel involved in the issuance of a Certificate must meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.4. Audit Logging Procedures

5.4.1 Types of Logged Events

All certificate services carried out within the certificate life cycle are logged. The following records relating to "e-tuğra"s "ECSP" operations and organizational functions are stored electronically and/or as hard copy and include the description, success/failure status and date of the event as well as information about the individuals related to the event:

- "ECSP" key (data) creation, back-up, storage, recovery, archiving and disposal.
- Cryptographic device lifecycle management events
- Certificate application, acceptance/rejection, validation, issuance, renewal, re-keying and revocation.
- Cryptographic device lifecycle management events
- Certificate and "CRL" creation and publication. and OCSP entries
- Successful or unauthorized access attempts to the PKI and other systems.
- System failures, hardware failures and other abnormalities
- All actions performed on systems.
- Staff entries to the "Trust Center" and exits from there.

- Firewall and router activities.
- Visitors' entries to the "ECSP" main facility and exits from there.

5.4.2. Log Processing Frequency

Audit logs are kept on a continuous basis and reviewed periodically. The audit records are backed up and archived at regular intervals.

5.4.3. Retention Period of Audit Logs

Once processed, audit logs are maintained and are accessible through the system according to the data processing storage capacity for at least 7 years. All data and documents that must be maintained according to applicable legislation are archived as described in Section 5.5.2.

5.4.4. Protection of Audit Logs

In order to protect audit logs, physical and logical access controls are used to prevent unauthorized viewing, modification, deletion or any other access to electronic and hard copy audit logs.

The data integrity of electronic audit logs is ensured through the keyed hashing method.

5.4.5. Audit Log Back-up Procedures

Audit logs are periodically backed up on-site at the "Trust Center" and off-site according to the applicable archive procedures.

5.4.6. Audit Data Collection System

At the time of application, the "ECSP" management application automatically generates and saves audit data for electronic actions at the network and operating system level. Audit data pertaining to manual actions are recorded manually by "e-tuğra" staff.

5.4.7. Notification to Parties Causing an Event

When the audit data collection system records a significant event, there is no need to warn the individual, organization or incumbent causing the event. However, depending on the essence and significance of the event the system notifies the senior manager(s) to whom the relevant individual reports.

5.4.8. Security Vulnerability Assessments

Routine audit log reviews enable the identification of security vulnerabilities in the system and procedures. Appropriate action is taken in case of any vulnerability.

Log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

"e-tuğra" performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process as discussed on section 8. "

5.5. Records Archival

5.5.1. Types of Records Archived

The following documents and data are backed up and archived according to "e-tuğra"s archive procedures:

- All applications for certificate processes, application agreements, and other relevant agreements and documents.
- Actions and data relating to the issuance, revocation, suspension and renewal of certificates (including the date of the actions and authorized persons carrying out such actions).
- Agreements and major correspondences with customers and business partners.
- All audit logs provided in Section 5.4.
- All certificates and "CRLs".
- "ECSP" root and intermediate certificates after their expiry.
- Requests and verification of requests for revocation, suspension, and removal of suspension as well as the relevant contact information.
- All "CPS" and "CP" documentation published by "e-tuğra" (all published versions).
- All procedures, instructions and forms used by "e-tuğra".

While some archives are kept electronically printed correspondences, forms, documents, customer records, company documents etc. are archived as hard copy. Records can be maintained electronically or as hard copy provided that they are arranged, stored, protected and reproduced in full and properly.

5.5.2. Archive Retention Period

Pursuant to the "Regulation" and applicable legislation, the records pertaining to "QECs" laid down in Section 5.5.1 must be kept for a period of not less than 20 years.

Records pertaining to Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC laid down in Section 5.5.1 must be kept for a period of not less than 10 years.

5.5.3. Protection of Archives

Electronically archived data is protected against any unauthorized viewing, modification, deletion or other access by using physical and logical access controls.

Data entered manually on hard copy documents is protected in physically protected areas accessible only by authorized staff.

5.5.4. Archive Back-up Procedures

As deemed appropriate, "e-tuğra" may keep the back-ups of documents and data on-site at the "Trust Center" and/or off-site, provided that the security level is the same as that of the originals.

Hard copy archives are not backed up.

5.5.5. Time-stamping Requirements for Records

CRLs, other database revocation inputs and any other data and documents deemed necessary by “e-tuğra” contain a time-stamp. Used time data is synchronized with UTC. All records are time-stamped as deemed necessary.

5.5.6. Archive Collection System

The archives are compiled electronically using the “e-tuğra” management systems or manually by authorized persons.

5.5.7. Archive Data Access and Verification Procedures

“CPS” and “CP” documents as well as sample end user agreements are published in the related section of the website (repository). Only “trusted staff” and Information and Communications Technologies Authority officials have access to classified documents. Certificate applications and data pertaining to subscribers and other data can only be accessed by duly authorized corporate applicants, provided that such data is relevant to their entity, “trusted staff”, registration officers, and Information and Communications Technologies Authority officials.

Documents available in the archive shall be kept in a readable format throughout their retention period.

5.6. Key Changeover

Pursuant to the relevant legislation, “e-tuğra” “ECSP” root and intermediate certificates shall be valid for not more than 10 years. As deemed necessary for security purposes the validity of the root and intermediate certificates may be extended before their expiration. For continuity of ECSP services, new “ECSP” root and intermediate key pairs and certificates are created at least 4 years before existing root and intermediate certificates expiration date. The previous keys are stored in a usable manner until the end of the validity. New certificates created after the “ECSP” root and intermediate certificate changeover are signed with new intermediate certificates. However, for the purposes of verifying previous certificates, access is made available to previous “ECSP” root and intermediate certificates.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Hazard Handling Procedures

Where incidents that affect security of “ECSP” operations occur, all necessary measures are taken in accordance with the “Business Continuity Plan”, “Disaster Recovery Plan”, and other data security management system procedures to resume the safe operation of the system, notify the affected parties and implement all other measures as soon as possible.

Subscribers and third parties can complete the Troubleshooting and Problem Form available on “e-tuğra”s website to solve any security problems they may encounter while using the certificates. “e-tuğra” assesses all reports made through the website and takes action as needed and provides feedback as soon as possible.

5.7.2. Hardware, Software and/or Data Corruption

Where the hardware, software and necessary data in the “Trust Center” is corrupted the back-up hardware and software is initially put into operation. Where data is lost the back-ups are put into

operation and/or re-created according to the “Business Continuity Plan” and “Disaster Recovery Plan”. If the certificate management processes are irreversibly damaged due to unrescuable data the certificates affected from the breakdown are immediately revoked, then new certificates are issued and the relevant parties are notified.

5.7.3. Entity Private Key Compromise Procedures

Where the security of private key in “e-tuğra” “ECSP” root and intermediate certificates is compromised, all relevant certificates are immediately revoked and all relevant parties are notified via the website and email according to the “Business Continuity Plan” and “Disaster Recovery Plan”. If appropriate, “e-tuğra” contacts government agencies, law enforcement, application software suppliers and other interested parties with predefined channels and activate any other appropriate additional security measures;

New private key for “e-tuğra” “ECSP” root certificates is then generated accordingly. Pursuant to applicable procedures, revoked certificates are replaced with new certificates.

5.7.4. Post-Disaster Business Continuity

In line with the “Business Continuity Plan” and “Disaster Recovery Plan” “e-tuğra” identifies the actions to be taken in the event of incidents that may prevent its operation.

Accordingly, “e-tuğra” has established Disaster Recovery Centers (DRC) outside of the “Trust Center”. In case of a disaster the critical and required data stored at the “Trust Center” is backed up to ensure business continuity. In particular, real time web services such as “OCSPs” and “CRLs” can be made available within 72 hours at the latest through the DRC in case such a need arises. Similarly, suspension, revocation and other similar certificate services can be made available 24 hours 7 days through the DRC without business interruption. Periodic drills are carried out for this purpose. In case of any security incidents that affect the certificates, operations action is taken in accordance with the “Business Continuity Plan”.

5.8. CA or RA termination

Where “e-tuğra” is obliged to terminate its operations, it shall notify the Information and Communications Technologies Authority of such termination and make a public announcement at least three months in advance pursuant to the applicable “Law” and “Regulation”. According to the procedures, “e-tuğra” shall hand over all data, documents and records pertaining to current “QECs” to another “ECSP” designated by “e-tuğra” or the Authority within one month pursuant to the Law. The Information and Communications Technologies Authority may extend this period by one month if deemed necessary and appropriate.

If the handover is not completed within the designated deadlines “e-tuğra” shall revoke all relevant certificates and notify all relevant parties through a public release and direct emails to subscribers and corporate applicants. In such a case, “e-tuğra” shall destroy its own private key and back-ups after all certificates are revoked and “CRL” logs are generated.

Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC subscribers shall be deemed duly notified of the termination through the public release and e-mailing. Similar to the mandatory handover for “QECs”, an attempt shall be made to handover these certificates. In this context, the clauses pertaining to “e-tuğra”s obligations and the issuance of status information for certificates that are still valid shall be regulated in the handover process.

All provisions in this article apply solely to active parties.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The process of generating key pair for e-tuğra's root and intermediate certificates is carried out by at least two pre-chosen and trained "trusted staff" and relevant officials by the use of secure systems that ensure the necessary security and cryptography for the generated keys, and in accordance with the procedures in a technically and administratively secured environment as described in section 5.2.2. Cryptography modules that are used to generate key pairs for e-tuğra's root certificate meet the conditions of FIPS 140-2 Level 3. Digital signing and key pairs of e-tuğra's root and intermediate certificates are generated in accordance with the algorithms and standards stated in ETSI EN 319 411-1, Baseline Requirements, EV Guidelines documents; and the "Communiqué"; the activities done during the key generation process are recorded and signed together with the date. These records are kept for audit and monitoring. An external auditor witness is required in generation of any CA keys to be used as publicly trusted root Certificates. The key pair is generated at a secure electronic signature creation device of "ECSP" and cannot be taken out except for the aim of backup. In order to keep data of key pair in safe condition, all necessary physical and technical safety measures are taken.

The key pair data of e-tuğra's root certificate are generated within the borders of the Republic of Turkey and they cannot be taken out of these borders in any condition. The validity period of key pair data of e-tuğra cannot exceed 10 years.

"e-tuğra" hardware security modules are kept and run under physical and electronic protection against all types of interference. Backup of data on modules are taken and stored in a safe according to the procedures. The keys on a module that physically need to be replaced, are terminated as stated in section 6.2.10 and the backups that will be used in new modules are stored in a different secure environment.

According to e-tuğra's "ECSP" working model, key pair for QECs belonging to certificate owner will be generated by e-tuğra in the places belonging to "ECSP" in accordance with algorithms and standards stated in the Article 6 of the Communiqué. The private key is generated within the secure electronic signature creation device at least has a standard of EAL+ according to ISO/IEC 15408 (-1, -2, -3) by a software able to give secure access and by "trusted staff". "e-tuğra" does not take a copy of the private key belonging to the certificate owner and/or it is not kept by e-tuğra.

Server administrators who apply for server certificates and technical administrators who apply for "CSC" are responsible for conducting the key generation securely.

6.1.2. Private Key Delivery to Certificate Owner

The signature creation and verification data (private and public key) for QEC owners can be generated in a secure electronic signature creation device and supplied to certificate owners together with QEC. Minimum "Secure Electronic Signature Creation Device and signature creation and verification data in this device and "Secure e-signature package" with QEC in it, are delivered to QEC owner by courier in exchange for his/her signature and identity control; to the certificate owner him/herself at RAs or at e-tuğra's center. In addition to this, the access data necessary for using secure electronic signature creation device is also supplied to certificate owner through call center or by courier or via online modules on the e-tuğra website.

Certificate application owners who will apply for Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC are responsible for a secure key generation during application. “e-tugra” does not generate Private Keys for publicly trusted SSL certificates.

6.1.3. Public Key Delivery to “ECSP

For QEC, key pairs are generated in a signature creation device and the private key is not archived by e-tuğra.

In cases where key pairs are generated by the certificate application owner, certificate request has to be signed by the private key. In order to provide the security of the requested information and to prevent third parties accessing the requested information, the request should be sent to e-tuğra via secure electronic communications.

6.1.4. “ECSP” Public Key Delivery to Users

“ECSP” certificates of e-tuğra (root and intermediate certificates) are published at http://www.e-tugra.com.tr/crt. SHA-1 and/or SHA-2 values of these certificates are published in three (3) most circulated national newspapers.

6.1.5. Key Sizes

“e-tuğra” selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the SSL Baseline Requirements, EV Guidelines and 5070 laws of the Turkish Republic for QEC.

Certificates must meet the following requirements for algorithm type and key size

Root CA Certificates	
Digest algorithm	SHA-256, SHA-384 or SHA- 512
Minimum RSA modulus size (bits)	4096
ECC curve	NIST P-256, P-384, or P-521
Subordinate Certificates	
Digest algorithm	SHA-256, SHA-384 or SHA512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
Subscriber Certificates	
Digest algorithm	SHA-256, SHA-384 or SHA512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

The information about the digest algorithm used in certificates issued by e-tuğra is given in section 7.1.3.

6.1.6. Parameters for Key Generation and Quality Checking

Key pairs belonging to e-tuğra’s root certificates and QECs are generated by “trusted staff” at e-tuğra’s Trust Center or at authorized RAs where physical and technical security conditions are fulfilled.

Parameters, algorithms and devices used during the generation process are in accordance with the requirements in the Communiqué.

Where key generation takes place on the applicant side for Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC, the applicant is responsible for generating the private key in appropriate tools and quality. “e-tuğra” checks and verifies the validity of the CSR file sent by the applicant according to key length and other parameters. ”e-tuğra” controls the received CSR file and rejects if it is signed with a 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 certificates issued by e-tuğra are only used for verification of signature, identification and authentication.

Keys of subordinate certificates of e-tuğra are used for signing user certificates, “CRLs”, “OCSP” certificates and time stamp certificates. Usage purposes of keys are indicated in key usage fields of certificates.

Keys of OCSP server certificates of “e-tuğra” shall be used for signing OCSP responses.

CA Certificates are not used to sign Certificates except in the following

cases:

- Self-signed Certificates to represent the Root CA itself;
- Certificates for Subordinate CAs and Cross Certificates;
- Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates; and
- Certificates for OCSP Response verification

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

“e-tuğra” uses secure electronic signature creation devices conforming to the standards specified in the Communiqué for key pair generation of QECs and CRL signing operations.

“e-tuğra” uses secure cryptographic hardware modules, i.e. HSMs certified at FIPS 140-1 Level 3 to protect signature generation, storage for private key and public key for root and intermediate certificates.

During the whole lifetime of cryptographic hardware modules, the devices are kept under continuous control regarding their functionality and any possible security incident is managed according to the related management procedure.

Private keys in the secure electronic creation devices are prevented from removal, export, modification or copying.

6.2.2. Private Key (n*m) Multi-Person Control

The access to e-tuğra “ECSP” private key and public key can be conducted by more than one “secure staff” performing necessary security and identification procedures. 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.

The access to cryptographic modules where private keys of root and intermediate certificates take place is allowed only by the presence of two authorized persons in a trusted role at the same time.

Private keys of QECs are only under the responsibility of certificate owners and they are stored in the password controlled, secure electronic signature creation devices.

6.2.3. Private Key Escrow

"e-tuğra" does not give "ECSP" private keys to any third party, even if the request for access is for official purposes. E-tuğra does not keep or copy private keys of end user certificates.

6.2.4. Private Key Backup

"e-tuğra" keeps copies of "ECSP" private keys for routine purposes and for protection against disasters. These data are backed up in cryptographic hardware modules and the relevant key storage devices by taking necessary technical and physical security measures, in secure hardwares that are EAL 4+ or FIPS 140-2 Level 3 certified in an encrypted form according to key generation and backup procedures. These backup copies are kept in safety boxes outside of the "Trust Center".

In cases when there is a need for key recovery, these backup copies are brought by e-tuğra's authorized signatory and they can be used only by authorized persons to reload the private keys into the relevant cryptographic hardware modules. These backup and recovery operations for private keys are conducted under the presence of at least two authorized personnel on trusted roles, in a technically and administratively secured environment by the entry of necessary access information.

Private keys of end user certificates are not backed up.

6.2.5. Private Key Archival

Private keys related to e-tuğra "ECSP" root and intermediate certificates are not kept for the purpose of forming archives. On the other hand, public keys are kept for further possible conflicts for 20 years. "e-tuğra" does not keep private keys of certificate owners in order to form archives.

6.2.6. Private Key Transfer into or from a Cryptographic Module

"e-tuğra" generates private keys of "ECSP" root and intermediate certificates 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 transfer of private key for backup purposes to another cryptographic module can be conducted under the presence of at least two trusted personnel, in a technically and administratively secured environment. If a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then all certificates that include the Public Key corresponding to the communicated Private Key are revoked by "e-tuğra".

Private keys belonging to QEC owners are generated within a secure electronic signature generation device and they cannot be taken out from there.

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

6.2.7. Private Key Storage on Cryptographic Module

Private keys of root and intermediate certificates of e-tuğra are stored on cryptographic hardware modules where they are generated and which have security levels specified in the Communiqué.

Private keys of QEC owners are stored on cryptographic hardware modules where they are generated and which have security levels specified in the Communiqué. Private keys in the secure electronic signature generation device are prevented from removal and modification.

6.2.8. Method of Activating Private Key

The activation of private keys of e-tuğra's root and intermediate certificates can be conducted in the presence of more than one authorized "trusted staff", under appropriate technical and physical security measures, by the entry of necessary access information.

The activation of private keys of QECs is done by entering a password to the secure electronic signature creation device and it is under the responsibility of the certificate owner.

The activation of private keys of Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC is done on the software and hardware of the certificate owner and it is under the responsibility of the certificate owner.

The certificate owner is responsible for an unauthorized use of the activation data by third parties and for taking necessary measures to prevent data theft or loss.

6.2.9. Method of Deactivating Private Key

Private keys of e-tuğra's root certificates are kept active only during its usage, when the usage is completed, they are out of active status.

When the secure electronic signature generation device of the private key data belonging to the QEC owner is out of the system or the secure electronic generation device is not used for a certain period of time while it was connected to the system, the activation is ended.

6.2.10. Method of Destroying Private Key

Private keys and backups of e-tuğra's root certificates are destroyed upon expiry of the validity term of the certificate or because of necessary technical and security measures, only by multiple authorized "trusted staff" under appropriate technical and physical measures; the operations performed are logged according to the procedures.

The destruction of private keys of QECs is dependent on the technical capability of the secure electronic signature creation device. Private keys of QEC can be destroyed by deleting data or by destroying the hardware.

Private keys belonging to certificates of Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC are under the responsibility of the certificate owner.

6.2.11. Operational Limits of Cryptographic Module

Private keys of e-tuğra and of QEC owners are generated and stored according to the security level specified in the Communiqué.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

"e-tuğra" root and intermediate certificates, end user certificates and relevant public keys are stored for at least 20 years. During this storage period, all necessary measures are taken in order to ensure the data integrity.

6.3.2. Operational Period of the Certificate and Key Pair Usage Period

The validity term of certificates ends upon the expiry date or when it is revoked. The validity period of the key pair is the same as the relevant certificate, but the public key can be used for the verification of the signature. The validity terms of e-tuğra's certificates are determined at the certificate application by certificate owner, corporate application owner and/or the authorized person.

"e-tuğra" terminates the functionality of the private key to sign certificates at an appropriate date before the validity term of the certificate ends.

The validity term of e-tuğra's root certificates cannot exceed 25 (twenty-five) years. If QEC certificates are issued from any of subordinated CA then it cannot exceed 10(ten) years.

The validity term of e-tuğra's intermediate certificates cannot exceed 10(ten) years.

The validity term for QECs is 1 (one) year, 2 (two) years or 3 (three) years and it cannot exceed 39 (thirty-nine) months.

The validity term for Standard, Premium and EV SSL certificates is 1 (one) year and it cannot exceed 13 (thirteen) months.

The validity term for CSC and EV CSC is 1 (one) year, 2 (two) years or 3 (three) years and it cannot exceed 39 (thirty-nine) months.

The validity term for other certificates cannot exceed 1 (one) and it cannot exceed 13 months.

6.4. Activation Data

Activation data are passwords and access codes used by "trusted staff" in operations requiring technical security; passwords for cryptographic modules where private keys of root and intermediate certificates take place, passwords for activation data about the usage of keys and passwords used by QEC owners to access private keys.

6.4.1. Activation Data Generation and Installation

The generation of the keys of e-tuğra's root and intermediate certificates and the creation of access codes to them is done according to the ceremony described in the relevant e-tuğra procedure. The use of private keys of root and intermediate certificates is described in section 6.2.2. Access codes consist of randomly determined for at least 8 (eight) alpha-numeric value and in a way not to include a meaningful word.

Activation data for QEC owners are generated by e-tuğra and are delivered only to certificate owners who can also create activation by themselves in a secure way via e-tuğra's website.

During activation, after the certificate owner passes security measures, an activation code for sole use is created for that moment in order to access the certificate or the smart card and it is notified to the certificate owner by an SMS to his/her mobile phone or by an e-mail to his/her e-mail address.

Certificate owners of Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC are responsible for creation and protection of the access passwords belonging to their certificate keys.

Owner of the activation data may change at any time under their control.

6.4.2. Activation Data Protection

After delivering the activation data to QEC owners and "trusted staff", the responsibility of protection and security of data secrecy belongs to QEC owners and "trusted staff".

Private keys belonging to e-tuğra root and intermediate certificates are stored according to procedures.

While creating their access passwords, e-tuğra recommends that an access password should be at least 6 (six) characters long, a character in it should not be repeated, not to use birth date, name and data which can be easily guessed. E-tuğra recommends to change the activation data at least once in 6 (six) months and determine a new activation data to all certificate owners.

6.4.3. Other Aspects of Activation Data

Activation data given to QEC owners are delivered in the closed envelope via secure courier services in exchange for a handwritten signature of the certificate owner or via e-tuğra's website by completing required identity control procedures.

The delivery of e-tuğra access passwords is only valid for QEC owners. If this delivery is done via secure courier service, the certificate card and the envelope that contains the activation code are sent by two different courier companies in order to take a measure for not delivering both of them at the same time in case of an access by a third party.

In the activation method, the activation code is determined at the time of operation by the certificate owner. The communication with e-tuğra's server is conducted in an encrypted manner for security steps and controls. The activation code is for sole use.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

All tasks and operations carried out within the process of e-tuğra "ECSP" are performed in accordance with information security management requirements. "e-tuğra"s information security management requirements are met by the use of secure and licensed software and hardware, the containment of attack detection systems in the network, access and operation control through identification methods based on information and ownership, storage and backup of all necessary operations and records.

Including any workstation e-tuğra systems are configured according to security controls below:

1. Before giving permissions to systems or applications, the identity of the user is verified.

2. Authorization of the user is managed properly and access rights are limited to the roles assigned to authorized people.

3. Audit records are formed for all operations and they are backed up.

4. For critical security processes -domain based security integrity is applied.

"e-tuğra" enforces multi-factor authentication on any account capable of directly causing Certificate issuance.

"e-tuğra" follows the recommendations of CWA 14167-1 standard under continuous auditing of the Information and Communication Technologies Authority of Turkey.

6.5.2. Operational Limits of Computer Security

Not applicable.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

System development controls of e-tuğra's certificate life cycle are conducted according to quality management procedures of e-tuğra and risk reducing methods which arise as a result of TS ISO/IEC 27001 audits.

"e-tuğra" has mechanisms in place to control and monitor the acquisition and development of its CA systems. "e-tuğra" only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

6.6.2. Security Management Controls

"e-tuğra" executes routine internal audit procedures to ensure the safety of operations controls of certificate life cycle management; also, in accordance with the compliance controls for ISO / IEC 27001, subject to the supervision of the independent auditor for safety management controls once a year.

"e-tuğra" has mechanisms in place to control and monitor the security-related configurations of its CA systems. All system checks and monitors are performed according to predeveloped procedures and instructions in yearly, quarterly or monthly time plans.

6.6.3. Life-cycle Management Controls

Not applicable.

6.7. Network Security Controls

Key generation, certificate life cycle management and other systems of e-tuğra "Trust Center" have the required network security infrastructure. In providing network security, hardware such as firewalls, switches and routers are structured with necessary configurations. E-tuğra's "Network Security Management" is conducted according to "Network Management Procedures''. In case where RAs transmit data to the "Trust Center", an electronic environment, they use secure network connection. 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 systemic vulnerability and penetration tests.

Any kind of external access to the "e-tuğra" 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 by authorized networks that are present in the Trust Center.

Registration authorities under "e-tuğra" communicate records relating to their certification operations to "e-tuğra" over the Internet by secure network connection.

"e-tuğra" performs its operations regarding network security according to Communication and Operation Management Procedure, meeting the requirements of ETSI EN 319 411-1, Baseline Requirements, EV Guidelines and Network and Certificate System Security documents. These requirements can be listed generally as seen below;

- "e-tuğra" effectively regulates the administration of user account management, auditing and modification or removal of access rights of the personnel who have direct access to the CA system.

- In case of privilege change for some personnel in a 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 these 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 the 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 certification services of e-tuğra, electronic records for relevant 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 phase of preparing archives.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

"e-tuğra" certificate profiles are based on the documents "ISO/IEC 9594-8/ ITU-T Recommendation X.509: "Information Technology- Open Systems Interconnection-The Directory: Public –key and attribute certificate frameworks" and "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Besides, for QEC profile also follows the document "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" ("Qualified Electronic Certificate, CRL and OCSP Request/Response Message Profiles – April 2007") which was published by the Information and Communication Technologies Authority of Turkey.

On issuer field of certificates, "e-tuğra" is written as "O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş." or "E-Tugra EBG A.Ş.".

The details of the Signature Algorithm are given in section 7.1.3 and the details of the Issuer and Subject are given in section 7.1.4.

7.1.1. Version Numbers

Root and sub-root certificates and end user certificates issued by "e-tuğra" 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 Extension

On "e-tuğra" root certificates and QECs, all extensions supported in the X.509 V.3 (2000) and ETSI TS 101 862.

QECs contain the qualified electronic certificate extensions defined under the "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile" and "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" ("Qualified Electronic Certificate, CRL, and OCSP Request/Response Message Profiles – April 2007") documents.

"e-tuğra" certificates basically contain the following fields;

- **Serial Number:** is an unique number within issuer scope, and is a non-sequential number greater than 0 containing at least 64 bits of output from a CSPRNG
- **Start of Validity**: UTC time encoded in accordance with RFC 5280
- **End of Validity:** UTC time encoded in accordance with RFC 5280
- **Public Key:** Key value encoded in accordance with RFC 5280
- **Signature:** Signature value encoded in accordance with RFC 5280.

In all certificate types, the following extensions are contained by certificates as standard fields:

- **Authority Key Identifier:** Public key hash value of the issuer "e-tuğra" certificate.
- **Subject Key Identifier:** Public key hash value of the certificate.
- **Basic Constraints:** CA marked as "false".
- **CRL Distribution Points:** URL of the CRL signed by the issuer of the certificate.

- **Authority Information Access:** URL Addresses of the "e-tuğra" issuer certificate and the "e-tuğra" OCSP service.

7.1.2.1 Root Certificate

Root Certificates are issued by "e-tuğra" according to Baseline Requirements (BR) 7.1.2.1 and RFC 5280

7.1.2.2 Subordinate CA Certificate

Subordinate CA Certificates are issued by "e-tuğra" according to Baseline Requirements (BR) 7.1.2.2 and RFC 5280. e-tuğra ensures that any Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross- certificates that share a private key with a corresponding root certificate: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId, and e-tuğra no longer includes both the id-kp- serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

7.1.2.3 Extensions for Subscriber Certificates

Extensions for QECs

QECs issued by "e-tuğra" contains following fields in addition to the standard extensions:

Key Usage: Digital signature and nonrepudiation fields are set. Extension is marked as critical.

Certificate Policies:

- For QECs the value of the Policy Identifier is set as 2.16.792.3.0.4.1.1.1 ("e-tuğra" QECs OID),
- The value of the Policy Qualifier Info – CPS is set as http://www.e-tugra.com.tr/cps ,
- For QECs the value of the Policy Qualifier Info – User Notice is set as "Bu sertifika 5070 sayılı Elektronik İmza Kanunu'na göre nitelikli elektronik sertifikadır.".

Subject Alternative Name: (is optional) May contain the e-mail address of the subject.

Qualified Certificate Statements:

- OID for ETSI TS 101 862 accordance (0.4.0.1862.1.1),
- OID for Turkish Information Technologies and Telecommunications Authority accordance (2.16.792.1.61.0.1.5070.1.1),
- Optional monetary limit is used.

Extensions for Standard (DV) SSL, Premium (OV) SSL ve EV SSL

Standard (DV) SSL, Premium (OV) SSL and EV SSL certificates issued by "e-tuğra" contains following fields in addition to the standard extensions:

Key Usage: Signing, key encipherment, data encipherment fields are set. KeyCertSign & cRLSign values are not set. Extension is marked as critical.

Certificate Policies:

- For Standard (DV) SSL certificates Policy Identifier is set as
  - 2.16.792.3.0.4.1.1.2 ("e-tuğra" Standard (DV) SSL OID),
  - 2.23.140.1.2.1 (CAB Forum DV Policy)
- For Premium (OV) SSL certificates Policy Identifier is set as
  - 2.16.792.3.0.4.1.1.3 ("e-tuğra" Premium (OV) SSL OID),
  - 2.23.140.1.2.2 (CAB Forum OV Policy)
- For EV SSL certificates Policy Identifier is set as
  - 2.16.792.3.0.4.1.1.4 ("e-tuğra" EV SSL OID),

- 2.23.140.1.1 (CAB Forum EV Policy)
- The value of the Policy Qualifier Info – CPS is set as http://www.e-tugra.com/cps ,

Subject Alternative Name: Contain at least one domain name (Fully-Qualified Domain Name) of the subject on the server as a dNSName entry.

Extended Key Usage: Server Auth or/and client Auth values are set but. anyExtendedKeyUsage value is not set.

Extensions for CSC and EV CSC

CSCs issued by "e-tuğra" contain following fields in addition to the standard extensions:

Key Usage: Signing, non-repudiation fields are set. Extension is marked as critical.

Certificate Policies

- For CSC certificates Policy Identifier is set as 2.16.792.3.0.4.1.1.13 ("e-tuğra" CSC OID)
- For EV CSC certificates Policy Identifier is set as 2.16.792.3.0.4.1.1.14 ("e-tuğra" EV CSC OID)

Extended Key Usage: Code signing and commercial software publishing fields are set.

7.1.2.4 All Certificates

All other fields and extensions are set in accordance with RFC 5280.

7.1.3. Algorithm Object Identifiers

"e-tuğra" uses the following algorithms and indicates their object identifiers on signing certificates, with the condition of the complying the "regulation" subject to and the up-to-date documents "Guidelines for Issuance and Management of Extended Validation Certificates" and "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates," and other Guides published by "CA/Browser Forum" on http://www.CAB Forum.org,

- SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
- SHA384WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
- ECDSAWithSHA256 {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2 }
- ECDSAWithSHA384 {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }ECDSAWithSHA512 {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

7.1.4. Name Forms

Certificate names issued by "e-tuğra" conform to the format of X.500 distinguished names.

On issuer field, "e-tuğra" is written in "O" (organization) as value "O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. "

The content of the Certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280

The following values are used on the fields of QECs:

- **SERIAL NUMBER:** Unique national citizenship ID for Turkish citizens or country code and passport number for foreigners.
- **CN:** The exact full name of the subject person. (first name + second name (if exist) + surname).
- **C:** "TR" (constant)

- **L:** Subject's city of residence (optional).
- **O:** The organization where the subject works (optional).
- **OU:** The organizational unit where the subject works (optional).
- **T:** The occupational title of the subject or title on the organization if organization name is given (optional).

The following values are used on the fields of Standard (DV) SSL:

- **CN:** values explained in Section 3.1.5 of this document.
- **C:** Country code of the subject (optional).
- **S:** State or province of the subject (optional).
- **L**: Subject's city of residence (optional).
- **O**: the same value of "CN" field.
- **SAN**: Authorized Fully-Qualified Domain Names in section 3.2.7 & section 3.1.5

The following values are used on the fields of Premium (OV) SSL:

- **CN:** values explained in Section 3.1.5 of this document.
- **GivenName, FirstName:** values explained in Section 3.1.5 of this document.
- **C:** Country code of the subject.
- **S:** State or province of the subject (optional – Required if L is absent).
- **L**: Subject's city of residence (optional - – Required if S is absent).
- **O:** values explained in Section 3.1.5 of this document.
- **SAN**: Authorized Fully-Qualified Domain Names in section 3.2.7 & section 3.1.5

The following values are used on the fields of EV SSL:

- **CN**: values explained in Section 3.1.5 of this document.
- **O**. values explained in Section 3.1.5 of this document.
- **BUSINESS CATEGORY:** One of the values "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending on the category of the subject.
- **JURISDICTION OF INCORPORATION COUNTRY NAME:** The name of the country where the jurisdiction about the subject organization is in effect. It is specified using the applicable ISO country code.
- **JURISDICTION OF INCORPORATION STATE OR PROVINCE NAME:** The name of the state or province where the jurisdiction about the subject organization is in effect. If the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province or locality level, then this field is mandatory along with country info.
- **JURISDICTION OF INCORPORATION LOCALITY NAME:** The name of the city where the jurisdiction about the subject organization is in effect. If the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level, then this field is mandatory along with State/Province and Country.
- **SERIAL NUMBER:** The trade registry number or code of the subject organization, which is certifiable in accordance with the legislation in the country of the subject and unique number as explained in Section 3.1.5 of this document.
- **C:** Country code of the subject (According to section 9.2.6 [EVG])
- **S:** State or province of the subject (According to section 9.2.6 [EVG])
- **L:** Subject's city or town of residence (According to section 9.2.6 [EVG])
- **STREET ADDRESS:** The street address and number of the subject (According to section 9.2.6 [EVG]).
- **POSTAL CODE:** The postal code of the subject (According to section 9.2.6 [EVG]).
- **SAN**: Authorized Fully-Qualified Domain Names in section 3.2.7 & section 3.1.5

No other attributes mentioned in EVG 9.2 are allowed.

The following values are used on the fields of CSC:

- **SERIAL NUMBER:** The trade registry number or code of the subject organization, which is certifiable in accordance with the legislation in the country of the subject and unique number.
- **CN:** The exact full name of the subject, which is certifiable in accordance with the legislation in the country of the subject.
- **C:** Country code of the subject.
- **S:** State or province of the subject.
- **L:** Subject's city or town of residence (optional).
- **O**: The exact full name of the subject, which is certifiable in accordance with the legislation in the country of the subject.

The following values are used on the fields of EV CSC:

- **SERIAL NUMBER:** The trade registry number or code of the subject organization, which is certifiable in accordance with the legislation in the country of the subject and unique number.
- **CN:** The exact full name of the subject, which is certifiable in accordance with the legislation in the country of the subject.
- **C:** Country code of the subject. (According to section 9.2.6 [EVG])
- **S:** State or province of the subject. (According to section 9.2.6 [EVG])
- **L:** Subject's city of residence (According to section 9.2.6 [EVG])
- **O**: The exact full name of the subject, which is certifiable in accordance with the legislation in the country of the subject.
- **BUSINESS CATEGORY:** One of the values "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending on the category of the subject.
- **JURISDICTION OF INCORPORATION COUNTRY NAME:** The name of the country where the jurisdiction about the subject organization is in effect. It is specified using the applicable ISO country code.
- **JURISDICTION OF INCORPORATION STATE OR PROVINCE NAME:** The name of the state or province where the jurisdiction about the subject organization is in effect. If the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province or locality level, then this field is mandatory along with country info.
- **JURISDICTION OF INCORPORATION LOCALITY NAME:** The name of the city where the jurisdiction about the subject organization is in effect. If the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level, then this field is mandatory along with State/Province and Country.
- **STREET ADDRESS:** The street address and number of the subject (According to section 9.2.6 [EVG]) (optional).
- **POSTAL CODE:** The postal code of the subject (According to section 9.2.6 [EVG])

No other attributes mentioned in EVG 9.2 are allowed.

The following values are used on the fields of roots and subordinates:

- **CN:** an identifier for the certificate such that the certificate's Name is unique across all certificates and subject to its main purpose.
- **C:** "TR" (constant)
- **O**: value "O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş."

7.1.5. Name Constraints

No anonymity or pseudonyms shall be used in certificates. Unique national citizenship ID for Turkish citizens or country code and passport number for foreigners are used as a distinguishing feature in the names for QECs.

The anyExtendedKeyUsage KeyPurposeId MUST NOT appear within extended key usage field of subordinate CAs..

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then a technically constrained Subordinate CA Certificate includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

- For each dNSName in permittedSubtrees, the “e-tuğra” confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements section 3.2.2.4.
- For each iPAddress range in permittedSubtrees, “e-tuğra” confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
- For each DirectoryName in permittedSubtrees the “e-tuğra” confirms the Applicant’s and/or Subsidiary’s Organizational name(s) and location(s) such that end entity certificates issued from the subordinate CA Certificate will comply with section 7.1.2.4 and 7.1.2.5 of the Baseline Requirements. If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate specifies the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate includes within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate also includes within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate includes at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate includes a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate includes at least one dNSName in permittedSubtrees.

7.1.6. Certificate Policy Object Identifier

In the “certificate policy” extension of certificates, the relevant certificate policy object identifier number (OID) indicated in Section 1.2 of this document is used according to certificate type.

7.1.7. Usage of Policy Constraints Extension

On sub-root certificates, policy constraints extension may be contained if necessary.

7.1.8. Policy Qualifiers Syntax

In the “certificate policy” extension of certificates, the access URL information for the CPS document has been provided as policy qualifier.

For QECs, an expression meaning that "QC" published by "E-TUGRA" is a qualified electronic certificate is placed under Qc Statements-Statement ID as “Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır” (“This certificate is a qualified electronic certificate, in accordance with 5070 numbered Electronic Signature Law”). In addition to this, following object identifier regarding qualified certificate is placed in the same place: “2.16.792.1.61.0.1.5070.1.1”. The object identifier belonging to optional related "Signature Policy" in certificate policies’ extension of "QCs" can be placed.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2. "CRL" profile

"e-tuğra" arranges CRLs appropriate to RFC 5280. CRLs contain "e-tuğra" electronic signature, CRL's date of publication, date of publication for the next CRL, and serial numbers of revoked certificates and dates and times of revocation. CRLs for QC are in accordance with the document "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" ("Qualified Electronic Certificate, CRL, and OCSP Request/Response Message Profiles – April 2007") which was published by the Information and Communication Technologies Authority of Turkey.

7.2.1. Version Number

CRLs published by "e-tuğra" are prepared in accordance with the format ITU X.509 V.2. CRLs that may contain the following fields per requirements.

- **Issuer:** The Subject DN of the issuing CA
- **Effective date:** Date and Time
- **Next update:** Date and Time
- **Signature Algorithm**: Depending Issuer CN
  - sha-256WithRSAEncryption [1 2 840 113549 1 1 11];
  - sha-384WithRSAEncryption [1 2 840 113549 1 1];
  - sha-512WithRSAEncryption [1 2 840 113549 1 1 13];
  - ecdsa-with-sha256 [1 2 840 10045 4 3 2]; OR
  - ecdsa-with-sha384 [1 2 840 10045 4 3 3]
- **Signature Hash Algorithm:** sha256 etc. (Depending upon CA)
- **Serial Number(s):** List of revoked serial numbers
- **Revocation Date:** Date of Revocation

7.2.2. CRL and CRL Entry Extensions

On CRLs published by "e-tuğra", Extensions defined in RFC 5280 are used.

CRLs have the following extensions:

- **CRL Number:** İncreasing serial number for each CRL
- **Authority Key Identifier:** AKI of the issuing CA for chaining/validation requirements
- **ReasonCode:** Identifies the reason for the Certificate revocation.

The extension is present for a CRL entry for a Root CA or Subordinate CA Certificate, including Cross Certificates. Supported values are keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5).

The extension may be present for a CRL entry for a Subscriber end entity Certificate. Supported values are keyCompromise (1), affiliationChanged (3), superseded (4), certificateHold (6).

The value certificateHold (6) is not supported for SSL Certificates.

7.3. "OCSP" profile

OCSP is an uninterrupted on-line certificate status protocol. The OCSP responses are in accordance with the document "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan

2007" ("Qualified Electronic Certificate, CRL, and OCSP Request/Response Message Profiles – April 2007") which was published by the Information and Communication Technologies Authority of Turkey.

OCSP responses complies with the requirements of Baseline Requirements. "e-tugra" operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 / RFC 5019 and highlights this within the AIA extension via an OCSP responder URL.

"e-tuğra" issues OCSP responses with following fields:

- Responder ID SHA-1: Hash of responder's Public Key
- Produced Time: The time at which this response was signed
- Certificate Status: Certificate status referenced (good/revoked/unknown)
- ThisUpdate/NextUpdate: Recommended validity interval for the response
- Signature Algorithm: SHA1 RSA, SHA256 RSA etc. (depending upon product)
- Signature: Signature value generated by the responder
- Certificates: The OCSP Responder's Certificate

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

Following fields are supported:

- Revocation Reason Identifies the reason for the Certificate revocation. The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

"e-tuğra" responds "unknown" for Unissued Certificates

7.3.1. Version Number

RFC 2560 is supported.

7.3.2. "OCSP" Extensions

RFC 2560 is supported.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Pursuant to the provisions of the Electronic Signature legislation "e-tuğra"s "ECSP" services and operations are subject to audits carried out by the Information and Communications Technologies Authority. Furthermore, the Information and Communications Technologies Authority audits "e-tuğra"s compliance to applicable standards and legislation at least once every two years.

Pursuant to the ETSI EN 319 411-1 standard and TS ISO/IEC 27001 certification "e-tuğra"s "ECSP" processes are subject to audits for data security periodically. In addition, according to the TS ISO/IEC 27001 Information Security Management System certification risk assessments are performed. Consequently, business risks are analyzed and the security conditions and operating procedures needed are identified. The risk analysis is updated regularly and updated as needed.

Pursuant to Standard ETSI EN 319 411-1, the Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC processes are subject to audits by an authorized independent auditor.

In addition to the above compliance audits, "e-tuğra" staff continuously carry out internal audits.

8.1. Frequency or Circumstances of Assessment

The Information and Communications Technologies Authority decides on the frequency of the audits, which are conducted at least once every two years. During the audit, any request from the auditors to access all documents and records, management areas, buildings and extensions, collect written and oral information, take samples, and audit operations must be fulfilled.

The compliance audits for the TS ISO/IEC 27001 certification are carried out on an annual basis.

Pursuant to the ETSI EN 319 411-1 audit standard, Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC services are subject to full audits on an annual basis.

Apart from periodic internal audits, authorized "e-tuğra" staff may conduct internal audits as needed.

8.2. Identity/Qualifications of Assessor

The Information and Communications Technologies Authority's audits are carried out by authorized Agency personnel.

The compliance audit for the TS ISO/IEC 27001 certification is carried out by an authorized auditor.

The auditor to conduct the ETSI EN 319 411-1 audit must be competent in the areas of Public Key Infrastructure ("PKI") technology, information security systems and techniques, information technologies and security controls, and third-party independent reporting. In addition, the auditor conducted in accordance with any one of the ETSI standards) must accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;

Internal "e-tuğra" audits are carried out by authorized "e-tuğra" "trusted staff".

8.3. Assessor's Relationship to Assessed Entity

The Information and Communications Technologies Authority determines the principles and procedures governing the audits that it carries out.

The TS ISO/IEC 27001 certification audit is carried out by an independent auditor.

The ETSI EN 319 411-1audit is carried out by an independent and authorized auditor.

"e-tuğra"s "trusted staff" carry out internal "e-tuğra" audits.

8.4. Topics Covered by Assessment

The Information and Communications Technologies Authority carries out audits to determine whether "e-tuğra" fulfills its statutory obligations related to electronic signatures.

The TS ISO/IEC 27001 certification audits cover "e-tuğra"s "Trust Center" operations and "ECSP" operations.

The ETSI EN 319 411-1 audit covers all standard processes related to Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC services as well as the technical infrastructure and facilities used to deliver these services.

"e-tuğra"s internal audits cover all provisions related to controls laid down in the ISO/IEC 27001 and ETSI EN 319 411-1 standards.

8.5. Actions Taken as a Result of Deficiency

In the event that any non-conformity is identified during "e-tuğra"s internal audits, the authorized "e-tuğra" staff shall take corrective and preventive action as soon as possible.

"e-tuğra" shall correct any minor non-conformities identified during the TS ISO/IEC 27001 audits until the next audit. The certificate shall be revoked in the case of any major non-conformity.

"e-tuğra" shall correct any minor non-conformities identified during the audits for compliance to the ETSI EN 319 411-1 standards until the next audit. The certificate may be revoked in the case of any major non-conformity, depending on the nature of the non-conformity.

If "e-tuğra" fails to fulfill its obligations arising from the legislation and applicable standards, as identified during the Information and Communications Technologies Authority's audits, the sanctions and penalties laid down in the applicable legislation shall be imposed on "e-tuğra".

8.6. Communication of Results

The results of the audit conducted by the Information and Communications Technologies Authority pursuant to the Law shall be officially notified to "e-tuğra" if deemed necessary. The absence of any feedback from the Authority shall be construed to mean that there is no negative assessment.

The auditing body conducting the TS ISO/IEC 27001 audits shall submit the results to "e-tuğra". The results of internal "e-tuğra" audits are submitted to the management team and relevant "trusted staff".

The auditing body conducting the ETSI EN 319-411-1 audits shall submit the results to "e-tuğra" and to the browsers via a letter that they accepted.

The results of internal "e-tuğra" audits are submitted to the management team and relevant "trusted staff". The results of internal audits are published in the internal audit reports and submitted to the relevant authorities for review.

8.7. Self-Audit

"e-tuğra" performs regular internal audits for validations against a randomly selected sample of at least three percent of its server and code signing Certificates Certificate types certificates issued since the last on quarterly basis, internal audit. Self-audits on these Certificates are performed in accordance with Guidelines adopted by the CA / Browser Forum.
Internal audit is applied for QEC validation twice in a year with a randomly selected sample set of certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance and Renewal Fees

Certificates issued by "e-tuğra" are priced according to their validity, the extent of the material transactions limits, the issuance costs, and market conditions. The material transaction limits and certificate financial and commercial general liability insurance premiums are reflected in the certificate prices. Current certificate fees are published on "e-tuğra"s website and other appropriate communication channels.

Pursuant to Article 13 of the Regulation on the Procedures and Principles for Implementing the Electronic Signature Law: in cases where "e-tuğra" revokes and renews qualified electronic certificates due to the theft and comprise of "e-tuğra"s root signature-creation data, lack of confidentiality or security or amended certificate principles that are not attributable to any fault on part of the subscriber, no fees shall be charged for renewals."

9.1.2. Certificate Access Fees

No access service fees shall be charged for certificates made publicly available by "e-tuğra" subscribers.

9.1.3. Revocation and Status Data Access Fees

"e-tuğra" communicates revocation and status data to the relevant parties for the certificates it issues through "CRLs" and "OCSPs". "e-tuğra" does not charge any access fees for access to "CRLs" and "OCSPs".

9.1.4 Fees for Other Services

"e-tuğra" does not charge any fees for manuals and documents such as "CP", "CPS", subscriber and certificate user agreements that it publishes pursuant to applicable laws and practices. Fees applicable to all other value added products and services offered to customers are published on "e-tuğra"s website and through other communication channels.

"e-tuğra" does not allow usage of the documents except reproduction, distribution, and processing of its documents for the purpose of reviewing certificates or for certificate processes.

9.1.5. Refund Policy

"e-tuğra" does not refund certificate service fees.

Only in cases where the certificate contains information different than that on the application due to "e-tuğra", the certificate shall be revoked and a new certificate shall be issued upon application without any fee whatsoever.

The fee for the remaining validity of a revoked certificate, starting from the date of revocation, shall not be refunded or set-off.

Certificate applications that are rejected as a result of "e-tuğra"s conduct shall be refunded upon request.

9.2. Financial Responsibility

Pursuant to Article 13 of the Electronic Signature Law "e-tuğra" must carry mandatory certificate financial liability insurance for "QECs". In accordance with Article 6 of the "Certificate Mandatory Financial Liability", the mandatory financial liability insurance guarantees that the "ECSP" will be held legally liable for any damages that the relevant parties may incur in case the "ECSP" fails to use secure products and systems, implement services in a secure manner, and prevent the counterfeiting and alteration of its certificates.

Pursuant to the ETSI EN 319 411-1 and CAB Forum Documents standard "e-tuğra" carries commercial general liability insurance and professional liability insurance for Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC services.

9.2.1. Insurance Coverage

The mandatory financial liability insurance for "QECs" covers material damages that arise due to staff errors, negligence or lack of due diligence on part of the "ECSP". These include but are not limited to:

- The "ECSPs" failure to use secure products and systems, implement services in a secure manner, and prevent the counterfeiting and alteration of its certificates;
- Inaccurate information contained in the certificates due to the "ECSP";
- Errors arising from the "ECSPs" inaccurate or incomplete processing of the information provided by qualified electronic signature subscribers at the time of issuance;
- Failures to issue the certificates with due regard to the agreement between the "ECSP" and "QEC" subscribers.

Damages arising from one or more of the below circumstances are not covered by the insurance:

- War, hostilities, conflicts (with or without the declaration of war), revolution, uprising, and disciplinary military acts related to these;
- Ionizing radiation or radioactive contamination arising from any nuclear fuel or nuclear waste resulting from burned nuclear fuel or reasons attributable to these as well as disciplinary and military measures taken in response to such circumstances;
- Natural disasters such as earthquakes, volcanic eruptions, submarine earthquakes, floods, inundations and flash floods, and landslides;
- Problems arising from the decisions of public authorities not attributable to the "ECSP";
- Problems in the communications infrastructure as well as the data processing infrastructure over which the "ECSP" has no direct control;
- The use of the qualified electronic signature for illegal purposes by the signer;
- The use of qualified electronic certificates that have not been revoked by the "ECSP" after the insurance company or holder have been notified and which cause collateral or further damage;
- Failure to comply with the principles and technical standards laid down in relevant laws, regulations and communiqués.

Standard (DV) SSL, Premium (OV) SSL and EV SSL certificates are covered by commercial general liability insurance and professional liability insurance. The commercial general liability insurance covers legal liabilities for all types of damages arising directly or indirectly from SSL services. Professional liability/errors and omissions insurance cover legal liabilities for damages arising as a result of "e-tuğra"s professional activities in relation to the SSL services.

9.2.2. Other Assets

Not applicable.

9.2.3. Scope of Insurance or Warranties for End Users

See Section 9.2.1.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

Confidential information includes: all information and documents deemed confidential for data security purposes as part of “e-tuğra”s technical and operational activities; business plans; sales information; partnership agreements; all classified information and documents pertaining to the commercial activities of business partners; root and intermediate certificate private key; action logs; information pertaining to subscribers deemed “personal data” pursuant to the “Law”; audit and assessment records; all confidential information and documents related to the “Trust Center”; technical security data related to hardware and software; access passwords to on-site areas and devices; and, facility layout and interior design plans.

9.3.2. Non-Confidential Information

Non-confidential information includes: information such as “CPS” and “CP” documents that need to be made public pursuant to the Law and practices and which are available on “e-tuğra”s website and repository; certificates published by “e-tuğra” in a public directory upon the subscriber’s consent; “e-tuğra”s root and sub-root certificates; and “CRLs”.

9.3.3. Responsibility to Protect Confidential Information

All “e-tuğra” employees are responsible for protecting confidential information. In accordance with the security policies no person or third party other than the authorized is allowed to access confidential information. All employees must strictly abide by the procedures related to data security.

Pursuant to Article 12 of the Electronic Signature Law, as regards “QECs” no information other than that required to issue a certificate can be requested from the applicant or obtained without the consent of the applicant. In addition, the certificate cannot be stored in an environment accessible by third parties without the consent of the subscriber.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

“e-tuğra”, in the scope of the services provided and pursuant to its obligations by law, protects the personal information of subscribers and other participants.

9.4.2. Private Information

The information obtained from the subscriber at the time of application and which are not included in the certificate content and “CRLs” are private information.

9.4.3. Non-Private Information

Information made publicly available through certificates and “CRLs” are non-private information.

As regards “QECs”, “e-tuğra” cannot make a certificate publicly accessible without the subscriber’s consent.

9.4.5. Notice and Consent to Use Private Information

“e-tuğra” may use the certificate and the information obtained at the time of application for the purposes laid down in the “CPS”, “CP”, and subscriber commitment.

9.4.6. Disclosures for Judicial and Administrative Purposes

“e-tuğra” subscribers and relevant parties agree that “e-tuğra” is authorized to disclose confidential/private information to competent authorities pursuant to applicable legislation provided that such a request is placed by the respective competent authority in accordance with the applicable legislation.

During the audits carried out by the Information and Communications Technologies Authority “ECSPs” are legally obliged to present all information and documents requested by the respective officials.

As regards “QECs”, subscribers and relevant parties agree that, in good faith, “e-tuğra” is authorized to disclose confidential/private information in response to judicial, administrative and other legal requests during the investigation phase of civil and administrative cases such as subpoenas, investigation documents, mutual petitions, evidence, and other documents.

9.4.7. Disclosures in Other Circumstances

Not applicable.

9.5. Intellectual Property Rights

“e-tuğra” holds the intellectual property rights for all certificates and root certificates issued by “e-tuğra”, certificate revocation data, “CPS” and “CP” documents, user agreements, all documents produced by “e-tuğra”, all databases created by “e-tuğra”, websites owned by “e-tuğra”, and all text, and audio-visual content on its websites.

Certificate owners and corporate application owners reserve the rights (if any) to all commercial brands, service brands, service marks or commercial names and titles that they own and given in certificate applications.

9.6. Representations and Warranties

9.6.1. “ECSP” Responsibilities and Warranties

“e-tuğra” warrants that the contents of all issued certificates are accurate, the identity validation processes have been duly performed, the certificate has been issued and delivered to the applicant authorized to make an application, the certificate status data is updated and accurate, and that all requirements and obligations set forth in the “CP” and “CPS” shall be fulfilled.

“e-tuğra” warrants that it shall fulfill its obligations laid down in Article 10 and 14 of the Law and Regulation, respectively, to issue “QECs” as well as its obligations set forth in the ETSI EN 319 411-1 standard to deliver SSL certificate products.

As regards “QECs”, “e-tuğra” shall perform services related to issued electronic certificates, time stamps and electronic signatures in accordance with applicable legislation. The “ECSP” is liable to indemnify third parties in case of any damage incurred due to the violation of the “Law” or “Regulation” based on the “Law”. “e-tuğra” may limit its liabilities towards certificate subscribers and third parties only to the extent of the material transaction limits for the relevant certificate. “e-tuğra” shall not be held liable for any damage that may be incurred due to the use of the certificate beyond its material transaction and/or use limits set forth in the certificate. “e-tuğra” shall carry the mandatory financial liability insurance, as per Article 13 of the “Law”, to indemnify any damage that may occur because of its failure to perform its obligations arising from the “Law” and relevant legislation.

As regards EV SSL certificates “e-tuğra” warrants that, as of the date that the certificate was issued, the subject named in the certificate legally exists as a valid organization or entity and that its legal name matches official records. In short, “e-tuğra” warrants the legal existence and identity of the subject. To this end, “e-tuğra” has taken all necessary steps to verify that, as of the date that the certificate was issued, the subject named in the certificate has the exclusive rights to use all of the domain names listed in the certificate (Right to Use Domain Name) and has authorized the issuance of the certificate (Authorization) and has verified the accuracy of all other information contained in the certificate (Accuracy of Information). Accordingly, the subject named in the certificate shall enter into a legally valid and binding letter of commitment with “e-tuğra” that fulfills the requirements of the “CP” and “CPS” or the applicant’s representative shall duly acknowledge and accept the relevant terms and conditions.

The EV SSL certificate warranties apply to the below parties:

- The certificate subscriber entering into the EV SSL certificate user agreement;
- The subject named in the certificate;
- All application software suppliers with whom “e-tuğra” has agreed or entered into a contract to include its root certificate in the software distributed and/or operated by such application software suppliers;
- All third parties that rely on such certificates throughout its validity term.

As regards EV SSLs, “e-tuğra” fulfills the requirements of this “CPS” document and maintains a repository, accessible online 24/7, containing up-to-date information about the validity and revocation of its certificates. “e-tuğra” shall revoke EV SSL certificates in accordance with the provisions for revocation set forth in this “CPS” document and the CA-Browser Forum manual.

9.6.2. Registration Authority Responsibilities

“RAs” are responsible for taking certificate applications, validation of the certificate applicant’s identification and other information according to the certificate types as set forth in this “CPS” based on the necessary documents, obtaining the necessary information and documents from the certificate subscriber and submitting them to “e-tuğra”, and taking certificate renewal, suspension and revocation requests and submitting them to “e-tuğra”.

“RAs” authorized to issue key pairs for “QECs” are responsible for the security of such issuance.

“e-tuğra” is exclusively responsible towards certificate subscribers and third parties for the accuracy of the information contained in the certificates. The responsibility regime between “e-tuğra” and “RAs” that are not directly part of “e-tuğra”s organization are regulated under the “Registration Authority Service Agreement”.

“RAs” authorized for only processing QEC applications.

9.6.3. Certificate Subscriber and Corporate Applicant Responsibilities

Certificate owners are responsible for submitting accurate information and documents to “e-tuğra” at the time of certificate application, renewal and revocation, use their certificates in accordance with the terms and conditions set forth in the “CP” and “CPS” documents, and fulfill all obligations laid down in the certificate user agreement.

Certificate owners are responsible for checking the validity of their certificate prior to use, and refraining from using certificates that have expired, suspended or revoked.

“QEC” owners are responsible for using their certificate solely to create secure electronic signatures and for verification processes, ensure that no one else but the subscriber uses the private key, maintain the confidentiality of access data, use the certificate within the material transaction limits, ensure the confidentiality and security of the environment where the certificate is used, and use the certificate in accordance with the user agreement, ”CPS” and “CP”. Where “QEC” subscribers fail to perform the above-mentioned obligations and such failure leads or has led to any damage, the subscriber is responsible for duly indemnifying “e-tuğra”, third parties, and other relevant parties.

Corporate applicants are responsible for validation the identification of the “QEC” subscribers for whom it lodges a “QEC” application according to the documents set forth by “e-tuğra”, obtaining written consent from “QEC” applicants demonstrating their request to become “QEC” owners, and obtaining the information and documents determined by “e-tuğra” from the “QEC” applicants and submitting them to “e-tuğra”.

Corporate application owners are responsible for verification identification of persons for whom a “QEC” application is accurate and based on the “CP”, “CPS”, and official documents stated on the website. Where corporate application owners fail to perform the above-mentioned obligations and such failure leads or has led to any damage, the corporate application owner is responsible for duly indemnifying “e-tuğra”, third parties, “QEC” subscribers, and other relevant parties.

9.6.4. Third Party Responsibilities and Warranties

Third parties are responsible for verifying the secure electronic signature and checking the validity of the “QEC” before performing any action based on a secure electronic signature generated in association with a “QEC”. Third parties may fulfill this responsibility by using a “secure signature verification tool”. Third parties are also responsible for satisfying the obligations set forth in Article 16 of the “Regulation”.

Where third parties fail to perform the above-mentioned obligations and such failure leads or has led to any damage, the third party is responsible for duly indemnifying “e-tuğra”, certificate subscribers, corporate applicants, and other relevant parties.

Standard (DV) SSL, Premium (OV) SSL, EV SSL, CSC and EV CSC subscribers, and third parties are responsible for validating the content and validity of the certificates when accepting, using and ensuring the security of the certificates.

9.6.5. Responsibilities and Warranties of Other Participants

“e-tuğra” may enter into service agreements with third parties to deliver certain services during its “ECSP” operations. The responsibilities of third parties are determined as per the respective service agreement. Service agreements contain provisions guaranteeing that third parties shall not disclose “e-tuğra”s business processes and confidential or private information pertaining to its customers.

9.7. Disclaimers of Warranties

Not applicable.

9.8. Limitations of Liability

"e-tuğra"s liabilities are limited to the material transaction limits included in the certificate and the responsibilities set forth in the user agreement.

The mandatory certificate financial liability insurance for "QECs" covers a 10,000 TL per occurrence limit and a 1,000,000 TL maximum annual aggregate limit.

The commercial general liability insurance for Standard (DV) SSL, Premium (OV) SSL and CSC covers a 10,000 TL per occurrence limit and a 1,000,000 TL maximum annual aggregate limit.

The commercial general liability insurance for EV SSL and EV CSC certificates covers a 2.000.000 USD per occurrence limit and annual aggregate limit. The professional liability insurance covers a 5.000.000 USD per occurrence limit and annual aggregate limit.

9.9. Indemnities

Where certificate subscribers fail to perform their obligations under the user agreements, the subscriber is responsible for indemnifying any damage that e-tuğra", corporate application owners or third parties may incur.

Where QEC corporate application owners fail to perform their obligations under the Corporate Application Agreement, the corporate certificate subscribers are responsible for indemnifying any damage that e-tuğra", certificate subscribers, or third parties may incur.

Where there is official evidence that "e-tuğra" fails to perform its obligations under the "Law" and relevant legislation or according to the principles and practices in the "CPS" and "CP", "e-tuğra" is responsible for indemnifying any officially proven damage that certificate subscribers and third parties may incur due to such failure.

Where certificate subscribers fail to perform their obligations under the certificate subscriber commitment or agreement as well as the obligations set forth in the "CP" and "CPS" documents, the certificate subscriber should indemnify "e-tuğra" or third parties for any damage that they may incur due to such failure.

"e-tuğra" shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.10. Term and termination

9.10.1. Validity of the "CPS" Document

This "CPS" is valid from the date of publication in "e-tuğra"s repository and remains valid until a new version is available.

9.10.2. Termination of the "CPS" Document

This "CPS" shall become null and void as of the publication of a new version.

9.10.3. Effects of Termination and Survival

"e-tuğra" publicly communicates the effects of the expiration of the "CPS" document via the repository on its website. In any case, "e-tuğra"s obligations to protect confidential information continue. All User Agreements are valid until the revocation or expiration of a certificate. The new version of the "CPS" is produced before the former "CPS" expires and the replacement is made without any interruption of services. In case of any amendment to the certificates generated according to updated "CPS" documents, certificate subscribers and third parties shall be duly notified and the necessary actions taken.

9.11. Individual Notices and Communications with Participants

Communications from "e-tuğra" to certificate subscribers and corporate applicants are made by e-mail, telephone or in writing. Certificate subscribers communicate with "e-tuğra" using the contact information provided in Section 1.5.2.

Public releases or notices to third parties are made through "e-tuğra"s website, by e-mail or in writing.

If "e-tuğra" deems necessary, it may include notes and clauses regarding communications in the user agreements.

9.12. Amendments

Where an amendment needs to be made in the published version of the "CPS" document, the "CPS" document containing the amendments is published as a new version upon the approval of "e-tuğra"s Security Board.

While the new version may contain minor amendments that do not affect the certificates generated according to the previous "CPS" there may also be major amendments that affect the current certificates. "e-tuğra" takes the necessary measures in case of any amendments that affect the use of certificates.

9.12.1. Amendment Procedure

"e-tuğra" 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.

In case of any amendment or update in "e-tuğra"s operations, "e-tuğra" updates such amendments in both "CP" and "CPS", and publishes as a new version.

In case of any amendment or update in the "CP" document the relevant sections of the "CPS" are updated. The "CPS" document is published as a new version. The "CPS" document and relevant practices are reviewed annually at the management review meetings and a new version of the CPS is published annually, even if no changes are made.

Where minor amendments are made to the "CP" and "CPS" documents the certificates issued prior to the update remain in force according to the new "CP" and "CPS" version. If a new "CP" and "CPS" version has been published due to major amendments, the certificates issued prior to the update and

which are associated with the amended "CP" and "CPS" may not be compatible with the new "CP" and "CPS".

9.12.2. Notification Mechanism and Period

"e-tuğra" shall notify the Information and Communications Technologies Authority of any amendments to the "CPS" within seven (7) days.

The new "CP" and "CPS" versions shall be made available to all relevant parties on "e-tuğra"s repository together with the older versions and detailed information about the version.

Articles Amendable without Notification

"e-tuğra" publishes amendments and/or corrections made on the "CP" and "CPS" that do not affect the rights and responsibilities of the related parties on its website without any prior notification.

"e-tuğra" is authorized to make any necessary amendments to the "CP" and "CPS" for the security of its operations without any prior notification. Amendments made in such cases become effective after the amendment and correction is published in the repository.

Articles Amendable with Notification

As regards "CP" and "CPS" amendments and/or corrections that affect the rights and responsibilities of the parties covered by the "CP" and "CPS", "e-tuğra" shall notify such amendments and/or corrections as a proposal/draft in advance as it deems appropriate depending on the significance of the amendments and/or corrections.

"e-tuğra" notifies certificate subscribers and other relevant parties of any proposals/drafts through its website. "e-tuğra" makes the necessary amendments taking into account the feedback received for the proposed/draft document within the given deadlines and enforces such amendment and/or correction upon publication in the repository.

9.12.3. Circumstances Requiring an Object Identifier Number Change

In cases where "e-tuğra" publishes a new certificate policy for use in a new certificate practice area or where the certificate policy's object identifier numbers need to be changed, the new certificates issued for use in the certificate field shall contain the object identifier numbers of the new certificate policy to be implemented.

9.13. Dispute Resolution Provisions

Settlement: In case of any dispute, problem or dissidence between "e-tuğra" and certificate subscribers or third parties, both parties shall notify the other party in writing and shall use the best endeavours to resolve the dispute in good faith in accordance with the principles and practices laid down in the "CP" and "CPS" documents as well as the procedures, commitments and agreements. The Regulation and Communiqués shall apply to any actions related to qualified electronic certificates.

Reconciliation: If within one (1) month of the dispute date one party documents to the other party in writing that such endeavours have failed, the parties' attorneys shall try to reconcile both parties, by virtue of their powers set forth in Article 35/A of the Legal Practitioner's Law, according to the principles and practices laid down in the "CP" and "CPS" documents as well as the procedures, commitments and agreements. The Law, Regulation and Communiqués shall apply to disputes related to qualified electronic certificates.

Arbitration: In cases where the parties' attorneys fail to reach reconciliation the Ankara Courts in Turkey shall have jurisdiction for the resolution of disputes.

9.14. Governing Law

As regards "QECs" the "CPS" shall be construed in the meaning of the Electronic Signature Law No. 5070 and the Communiqués.

The laws of the Republic of Turkey shall apply for the implementation and interpretation of the "CPS".

9.15. Compliance with Applicable Law

"e-tuğra" performs and implements its "QEC" services in accordance with the Electronic Signature Law No. 5070 and the relevant Regulations, Communiqués and other legislation.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Not applicable.

9.16.2. Assignment and Transfer

Not applicable.

9.16.3. Severability

Where any section of the "CPS" is deemed or becomes invalid permanently or temporarily, the other sections that are not affected from such section shall remain in force.

Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Sanctions (Waiver of Rights)

Not applicable.

9.16.5. Force Majeure

In case of force majeure "e-tuğra" may not be able to perform its obligations arising from the "CPS". Force majeure includes situations that prevent "e-tuğra" from performing its operations and are beyond its control under normal circumstances such as wars, mobilization, natural disasters, fires, failures in telecommunications lines, and circumstances such as legislation changes where, based on the principle of integrity, any demand to perform such change would impose a significant administrative and financial burden on the other party.

9.17. Other Provisions

Not applicable.