e-tuğra

CERTIFICATE POLICY

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
Version: 4.2
Validity Date: September, 2017
Update Date: 29/09/2017

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 Policy (CP)

Trademark Notices

Trademarks used in this document are registered trademarks under the ownership of E-Tuğra EBG Information Technologies and Services Corp. or relevant parties.

CONTENTS

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 Policy (to be referred to as "CP" 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 policies 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, CWA14167-3, 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.cabforum.org by "CA/Browser Forum" which are called "Guidelines for Issuance and Management of Extended Validation Certificates" and "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" for the services such as Standard SSL (Secure Socket Layer), Premium SSL, EV (Extended Validation) SSL Certificates and Code Signing Certificate.
- 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 and this CP we consult to the Regulation, Guidelines or ETSI documents.

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 bring this document to the attention of the public and the concerned parties. Policies 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.

1.2. Document Name and Identification

This "CP" document is called "e-tuğra Certificate Policy" and it is prepared in order to explain the certificate policies. The version number and the validity date take place on the cover page of the document.

"e-tuğra CP document" 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 SSL Certificate Policy
It covers SSL certificates for servers.
Object Identifier: 2.16.792.3.0.4.1.1.2 (corresponds to policy with OID: 0.4.0.2042.1.6)

"e-tuğra" Premium SSL Certificate Policy
It covers SSL certificates for servers.
Object Identifier: 2.16.792.3.0.4.1.1.3 (corresponds to policy with OID: 0.4.0.2042.1.7)

"e-tuğra" EV SSL Certificate Policy
It covers EV SSL certificates for servers.
Object Identifier: 2.16.792.3.0.4.1.1.4 (corresponds to policy with OID: 0.4.0.2042.1.4)

"e-tuğra" Code Signing Certificate Policy
It covers the certificates for code signing operations.
Object Identifier: 2.16.792.3.0.4.1.1.3 (corresponds to policy with OID: 0.4.0.2042.1.1)

"e-tuğra" EV Code Signing Certificate Policy
It covers the EV certificates for code signing operations.
Object Identifier: 2.16.792.3.0.4.1.1.4 (corresponds to policy with OID: 0.4.0.2042.1.7)

Standard SSL Certificates are issued and maintained according to the "Normalized Certificate Policy" and "Domain Validated Certificate policy" defined in ETSI EN 319 411-1.

Premium SSL Certificates are issued and maintained according to the "Normalized Certificate Policy" and "Organization Validated Certificate policy" defined in ETSI EN 319 411-1.

EV SSL Certificates are issued and maintained according to the “Normalized Certificate Policy” and “Extended Validated Certificate policy” defined in ETSI EN 319 411-1.

Code Signing Certificates are issued and maintained according to the “Normalized Certificate Policy” and EV Code Signing Certificates are issued and maintained according to the “Extended Validated Certificate Policy Guideless” defined in ETSI EN 319 411-1.

1.3. Participants

The subjects defined as Participants under “e-tuğra CP” 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 CP” 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 “CP” 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 ve 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 of 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 circle 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 relayed 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.

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 to 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 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 fulfill the requirements cited in e-tuğra's "CP" and "CPS" documents and in "Qualified Certificate Owner User Agreement" and whose certificate is issued.

1.3.4. 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.

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

1.3.5. Other Parties

In 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 "CP" and "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 kind 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 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 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 hold 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 signature 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 "CP" document.

1.5. Policy Administration

e-tuğra, as the authority that establishes the certificate policy is responsible of the management of this "CP" document.

1.5.1. Organization Administering the Document

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

1.5.2. Contact

Contact information for e-tuğra "CP" 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
Web: http://www.e-tugra.com.tr – http://www.e-tugra.com

1.5.3. Person Determining CP Suitability

The compability and applicability of this CP document to e-tuğra ECSP certificate processes is audited by authorized e-tuğra management board.

1.5.4. "CP" approval procedures

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

"e-tuğra" conforms to the current version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1" which is published by CA/Browser Forum at http://www.cabforum.org for all SSL certificates and conforms to the current version of "Guidelines for the Issuance and Management of Extended Validation Certificates" which is published by CA/Browser Forum at http://www.cabforum.org for EV SSL certificates. In case of any inconsistency between the Guidelines and this CPS, the Guidelines shall prevail.

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
“EVCP”	**“Extended Validation Certificate Policy”**
“EVCG”	**“Extended Validation Certificate Policy Guideless”**
"DRC"	Disaster Recovery Center
"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 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 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 on 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 key.**
"Law"	**Electronic Signature Law published on 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 SSL"	**The SSL certificate issued and maintained in accordance with OVCP in 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.
"Private 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 Authorly"	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 person 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 provide 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 of 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 signature.**
"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 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 service is not unavailable no longer than 24 hours.

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 are 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 and Certificate Agreements
- Corporate Application Agreements
- Documents related to certificate applications
- Informative documents and relevant audio and visual publications

The access to these information's referred to in this section are publicly disclosed at e-tuğra's website http://www.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.
- 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 "CP" 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.

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 certificate owner’s name in QECs, Premium SSL, EV SSL and CSCs.

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 owner 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 identity information of different people in QECs to be unique in all issued QECs.
- In standard SSL Certificates, distinguishing the certificate owner uniquely is achieved by the field name to which certificate is issued.
- In Premium and EV SSL Certificates, e-tuğra uses unique name field for all kind of legal entities resident in Turkey according to ”e-tugra” CPS.
- For Uniqueness of Name in Premium 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.
- Wildcards are not issued for Standart and EV SSL certificates

3.1.6. Recognition, Authentication and Role of Trademarks

"e-tugra" verifies the trademark stated in SSL certificate application forms. Verification of trademark is done according to related country's regulation and legislation.

"e-tugra" 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

3.2.1. Method to Prove Possession of Private Key

In other certificates, certificate applicants prove their possession of Private Key. 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

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 legal entity is conducted according to e-tuğra procedures which are dependent on the predetermined conditions.

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.

Premium 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.

EV SSL and EV CSC

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

- 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, circular of signature or another valid official document in applicable legislation is required in order to show that 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. 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 e-mail message to the authorized person.
- The domain name which will take place in the certificate should belong to the legal entity or the right and authority to use the domain name should 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".

Standard SSL

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

3.2.3. Authentication of Individual Identity

The identity of the people applying for QEC 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 on 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.

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 "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.

Other fields such as "L", "S", and "O" that may appear in 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 Standard SSL, the verification of domain name authority is made by a successful confirmation answer received from the contact information of the person in WHOIS records or from addresses webmaster@<domain_name>, postmaster@<domain_name>, admin@<domain_name>, administrator@<domain_name>, hostmaster@<domain_name>.

For Premium SSL, there is a need for an official document to support that the applicant has the authority to act on behalf of the legal entity.

For EV SSL, procedures prepared according to the “Guidelines for Issuance and Management of Extended Validation Certificates” published by “CA/Browser Forum” are applied.

3.2.6. Interoperability Criteria

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

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 is 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 central office address or via Registration Authorities. For re-key operations, there is no need to make face to face identification.

For certificates of Standard SSL, Premium SSL, EV SSL and “CSC” and “EV SSL” there is no possibility to re-key or to renew.

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 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 this “CP” and related “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.

In other kinds of certificates, 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.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

"e-tuğra" issues certificate and manages the certificate life-cycle in accordance with the policies set forth in this "CP" 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 applicant on behalf of their employees, customers, members or shareholders.

Any legal entity including public institutions and government agencies may apply for Standard SSL, Premium SSL, EV SSL, "CSC" and EV SSL.

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 owner may visit in person 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 applicant fills out and signs 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, or by completing the Certificate Application Form available on the web address of 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 polices and principles of Corporate Application Agreement signed between Corporate Applicant and "e-tuğra" behalf of e-tuğra. T

SSL Application:

The applications of Standard SSL, Premium 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.

For Premium SSL and EV SSL, 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. 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. 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 policies 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 SSL, Premium SSL, EV SSL CSC and EV CSC are conducted according to policies and relevant e-tuğra procedures explained in section 3.2.

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 policies 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 application of Standard SSL, Premium SSL, EV SSL and "CSC", CSR file is not delivered to e-tuğra.
- For a Standard SSL, Premium SSL, EV SSL and "CSC" application, there is a strong belief that issuing such certificate may endanger the reputation of e-tuğra.

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 SSL, in between 3 (three) and 6 (six) days for Premium 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 policies 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.

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 of the certificate issued by e-tuğra is deemed as the acceptance of the certificate. For all kind 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 are 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.

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 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.

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

"e-tuğra"s 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

Policies 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. Policies of section 4.4.1 apply.

4.6.6. Publication of Renewed Certificate by "ECSP"

Policies 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 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

Policies of section 4.3.2 apply.

4.7.5. Operations Deemed Acceptance of Re-keying of Certificate

Policies of the section 4.4.1 apply.

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

Policies 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 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

Policies 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

Policies of section 4.3.2 apply.

4.8.5. Operations Deemed Acceptance of Modified Certificate

Policies of section 4.4.1 apply.

4.8.6. Publication of the Modified Certificate by “ECSP”

Policies 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

The following circumstances require certificate revocation:

- The information included in the certificate is no longer valid during the validity term of the certificate.
- Request by the certificate owner or by the person authorized to represent which can be made via e-tuğra’s official website, call center, by sending e-mail and signing by secure electronic signature or in a written way.
- It is understood that the information in certificate or certificate application is false or incorrect; 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.
- 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.
- 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 unsecure.
- It is understood or notified 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.
- As a result of “e-tuğra”s sole discretion, during the administration of certificate, detecting non-compliance on the principles of related "CPS" guidebooks and on the policies of this "CP".
- For QEC, 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 is disappeared.
- Any of the algorithms, or associated parameters or key length, used when creating certificates are compromised or become insufficient for its remaining intended usage.

- If an evidence is obtained that the certificate was misused.
- It is understood that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name
- is discovered that the server certificate is being used to enable criminal activities such as phishing attacks, fraud or the distribution of malware.
- For QEC, 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.
- It is notified to e-tuğra or it is understood by e-tuğra that legal existence or business activity of the legal entity which is the applicant for Premium SSL and EV SSL certificates has been terminated.
- It is notified to e-tuğra or it is understood by e-tuğra that a court or an authorized person has received the authorization of use of certificate applicant's domain name for Premium SSL and EV SSL certificates.
- The right of e-tuğra to issue certificates for EV SSL is disappeared.
- There is a suspicion of revelation of private keys of e-tuğra's root and intermediate certificates or the fact that they are already aroused.
- E-tuğra suspends providing electronic certificate services.

Where a sub-root CA certificate loses its validity within the term of use, it shall be revoked within 7 (seven) days.

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 for Standard SSL,
- The authorized person to represent the certificate owner legal entity for Premium SSL, EV SSL and EV CSC,
- Public institutions and court authorities which have such authorization,
- E-tuğra staff in necessary circumstances.

4.9.3. Procedures for Revocation Request

"e-tuğra" gives certificate revocation service continuously on 7 days 24 hours basis via e-tuğra's website and call center. The requests made by a declarative statement written by the certificate

owner are processed within official working hours. For all type of SSL ve CSC certificates, revocation requests are taken only by call center or with declarative statements.

Revocation requests for QECs shall be received via different ways such as interactive operations on e-tuğra's website, call center and declarative statements written by the certificate owner (signed papers sent by fax or mail to e-tuğra or RAs). After this operation, the revocation status is notified to certificate and corporate application owner.

Revocation requests for Standard SSL may be achieved only by the completion of approval operations sent to e-mail addresses taking place in DNS records of the owner of the domain name.

Revocation requests for Premium SSL, EV SSL, "CSC" and EV CSC 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.

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 e-mail. 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 e-mail.

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.

Revocation requests received via written statement are taken into process immediately within the working hours and necessary operations are completed urgently.

Upon receiving the revocation request for SSL and CSC certificates revocation process is completed within 24 (twenty-four) hours.

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 proceed 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 is adequate to CWA 14171 Standards.

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

“CRLs” for QECs are published at least once every 24 hours, in order to be valid for 24 hours; “CRLs” for Standard SSL, Premium SSL, EV SSL and “CSCs” are published 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 user 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-tugra” 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-tugra” is signed using an OCSP responder certificate that is issued by the root or sub root certificate that issued the queried certificate.

“e-tugra” 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 Control Requirements

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

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

“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 effective again, the suspended QEC can be rendered effective again upon the removing 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 kind of certificates.

4.9.14. Who Can Apply for Suspension

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

4.9.15. Process of Certificate Suspension Requests

For QEC, policies 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 e-mail.

Suspension operations are not applied for other type 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 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 type 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

“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 7 days 24 hours. These services are not unavailable 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 to be 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 case 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.

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 Centre” that has various security areas designed to stop, prevent and detect covert or open attacks.

5.1.2. Physical Access

Physical access to “e-tuğra” “trust center” are always under control.

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 Centre” 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” “trust center” are equipped with appropriate insulation systems for protection against flooding.

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.

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 Centre” 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 Centre” 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 Centre 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

In general, “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 check 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 staff”s 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.

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 Centre” 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.

5.3.2. Professional Background Checks

A series of security and background checks are performed before “e-tuğra” general staffs and “trusted staff”s 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 private key infrastructure framework, Registration Authority and “Trust Centre” operations, “e-tuğra” security procedures, and certificate polices. “e-tuğra”s trainings are periodically revised and updated as needed.

5.3.4. Training Frequency and Conditions

In addition to the initial training, “e-tuğra” staff receives updated trainings at regular intervals. The frequency and content of the trainings are subject to change in line with the organization’s performance analyses. Trainings 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 unauthorised 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.

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.

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 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.
- Certificate application, renewal, re-keying and revocation.
- Certificate and "CRL" creation and publication.
- Successful or unauthorized access attempts to the system.
- System failures, hardware failures and other abnormalities.
- Staff entries to the "Trust Centre" 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 in and are accessible through the system according to the data processing storage capacity. 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 unauthorised viewing, modification, deletion or any other access to electronic and hard copy audit logs.

5.4.5. Audit Log Back-up Procedures

Audit logs are periodically backed up on-site at the “Trust Centre” 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.

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”.

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 SSL, Premium 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 unauthorised 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 Centre” 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.

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.

5.7.2. Hardware, Software and/or Data Corruption

Where the hardware, software and necessary data in the "Trust Centre" 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 is 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 e-mail according to the "Business Continuity Plan" and "Disaster Recovery Plan". New private key for "e-tuğra" "ECSP" root certificates is then generated accordingly.

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.

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 e-mails to subscribers and corporate applicants. In such case, "e-tuğra" shall destroy its own private key and back-ups after all certificates are revoked and "CRL" logs are generated.

Standard SSL, Premium 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.

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. The key pair is generated at 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 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 physical 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 that, at least has a standard of EAL+ according to ISO/IEC 15408 (-1, -2, -3) by a software able to give secure access opportunity and by "trusted staff". "e-tuğra" does not take a copy of private key belonging to 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 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 SSL, Premium SSL, EV SSL, CSC and EV CSC are responsible for a secure key generation during application.

6.1.3. Public Key Delivery to "ECSP

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

In cases where key pairs are generated by 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"s root certificates are issued by the use of 4096 bit RSA and intermediate certificates are issued by the use of 2048 bit RSA key pair.

Intermediate certificates used for QEC and "QEC"s are issued according to minimum key lengths specified in the Communiqué.

For certificates of Standard SSL, Premium SSL, EV SSL and "CSC" issued by e-tuğra 2048 bit RSA key pair is used.

The information about 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 generation process are in accordance with the requirements in the Communiqué.

Where key generation takes place on the applicant side for Standard SSL, Premium 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 CSR file sent by the applicant according to key length and other parameters.

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 root and intermediate 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.

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 life time 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 on 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 key to any third party, even if the request of 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 of 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 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.

Private keys belonging to QEC owners are generated within 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 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 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 SSL, Premium 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 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 SSL, Premium 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 at least for 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 key pair is the same as the relevant certificate, but 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 and 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 EV SSL certificates is 1 (one) year or 2 (two) years and it cannot exceed 27 (twenty seven) months.

The validity term for other certificates cannot exceed 1 (one), 2 (two) and 3 (three) years and it cannot exceed 39 (thirty nine) 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.

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.

Certificate owners of Standard SSL, Premium 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 in any time on 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) character 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 envelops 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 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 system in the network, access and operation control through identification methods based on information and ownership, storage and backup of all necessary operations and records.

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 e-tuğra's quality management procedures and risk reducing methods which arise as a result of TS ISO/IEC 27001 audits.

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.

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" in 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 systematic vulnerability and penetration tests.

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

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

"e-tugra" 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;

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.".

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 support on the X.509V.3 (2000) ve 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:** Unique number within issuer scope
- **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.

According to certificate type the following extensions are set if needed,

- **Key Usage**,
- **Certificate Policies,**
- **Subject Alternative Name**,
- **Extended Key Usage**.

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," published by "CA/Browser Forum" on http://www.cabforum.org,

- "SHA-1 with RSA" (1.2.840.113549.1.1.5),
- "SHA-256 with RSA" (1.2.840.113549.1.1.11),
- "SHA-384 with RSA" (1.2.840.113549.1.1.12),
- "SHA-512 with RSA" (1.2.840.113549.1.1.13).

For all subscriber certificates, SHA-256 algorithm is used. Root certificates which are for generating subscriber certificates still have SHA-1 or SHA-256 algorithm. But in all newly generated root and sub-root certificates SHA-256 algorithm is used, all new root and sub-root certificates are generated with SHA-256.

7.1.4. Name Forms

Certificate names issued by "e-tuğra" conform to the format on 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.

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.

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”.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2. “CRL” profile

“e-tuğra” arranges CRLs appropriate RFC 3280. 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 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.

7.2.2. CRL and CRL Entry Extensions

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

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.

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 SSL, Premium 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” staffs 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 SSL, Premium SSL, EV SSL, CSC and EV CSC services are subject to compliance audits on an annual basis and the certification is renewed every three years.

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 must be accredited by an official awarding body such as the European Cooperation for Accreditation for compliance to ISO/IEC 17021 and in accordance with Article 3.4 of the CEN Workshop Agreement (CWA) 14172-2 standard.

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 319 411-1 audit 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 Centre” operations and “ECSP” operations.

The ETSI EN 319 411-1 audit covers standard all processes related to standard SSL, premium 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 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.

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 certificate 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 CabForum Documents standard "e-tuğra" carries commercial general liability insurance and professional liability insurance for Standard SSL, Premium 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 SSL, Premium SSL and EV SSL certificates are covered by a 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 Centre"; 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" 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 certificate throughout its validity term.

As regards EV SSLs, "e-tuğra" fulfills the requirements of this "CP" 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 "CP" 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 "CP" 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".

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 it places 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 SSL, Premium 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.

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 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.

9.10. Term and termination

9.10.1. Validity of the "CPS" Document

This "CP" 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 "CP" Document

This "CP" 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 "CP" 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 "CP" is produced before the former "CP" expires and the replacement is made without

any interruption of services. In case of any amendment to the certificates generated according to updated “CP” 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 “CP” document, the “CP” 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 “CP” 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-tugra” evaluates its Certificate Policy 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, this document is revised if necessary.

In case of any amendment or update in “e-tuğra”s operations, “e-tuğra” updates such amendments in the “CP” 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.

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” version has been published due to major amendments, the certificates issued prior to the update and which are associated with the amended certificate policies may not be compatible with the new “CP” and “CPS”.

9.12.2. Notification Mechanism and Period

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” 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 amendments and/or corrections that affect the rights and responsibilities of the parties covered by the "CP" "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 on Turkey shall have jurisdiction for the resolution of disputes.

9.14. Governing Law

As regards "QECs" the "CP" 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 "CP".

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

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 "CP". 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.