e-tuğra

PDS
(PKI Disclosure Statement)

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
(E-Tugra EBG Information Technologies and Services Corp.)
Version: 1.0
Validity Date: January, 2018
Update Date: 26/01/2018

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.) PKI Disclosure Statement (PDS)

Trademark Notices

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 is a PKI Disclosure Statement following the structure of ETSI EN 319 411-1 (Annex A). It is a supplemental instrument of disclosure and notice by “e-Tugra” to Subscribers and Relying Parties and does not replace or substitute the latest version of “e-tugra” Certificate Policy and Certification Practice Statement (CP/CPS), published at https://www.e-tugra.com/CPS.

2. Contacts

2.1. General Contacts

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

2.2. Contact Information for Problem Reporting and Revocation

Technical Support: 0-850-532 23 12
E-Mail: destek@e-tugra.com.tr
Web: https://helpdesk.e-tugra.com.tr/

See sections 4.9.3of the “e-tugra” CP/CPS for revocation process.

3. Certification Type, Validation Procedures And Usages

Certificate Type	Policy Identifier	Policy OIDs	Short Description	Vaildation Procedures
Personel				
QEC	QCP	2.16.792.3.0.4.1.1.1	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.	All validation policy is explaind in CP/CPS section 3.1, 3.2
Server Certificates				
Standart SSL	NCP + DVCP	2.16.792.3.0.4.1.1.2 (corresponds to policy with OID: 0.4.0.2042.1.6)	It covers SSL certificates for servers.	All validation policy is explaind in CP/CPS section 3.1, 3.2
Premimum SSL	NCP + OVCP	2.16.792.3.0.4.1.1.3 (corresponds to policy with OID: 0.4.0.2042.1.7)	It covers SSL certificates for servers.	
EV SSL	EVCP	2.16.792.3.0.4.1.1.4 (corresponds to policy with OID: 0.4.0.2042.1.4)	It covers SSL certificates for servers.	
Code Signing				
Code Signing	NCP + OVCP	2.16.792.3.0.4.1.1.3 (corresponds to policy with OID: 0.4.0.2042.1.1)	It covers the certificates for code signing operations	All validation policy is explaind in CP/CPS section 3.1, 3.2
EV Code Signing	EVCG	2.16.792.3.0.4.1.1.4 (corresponds to policy with OID: 0.4.0.2042.1.7)	It covers the certificates for code signing operations	

4. Relience Limits

“e-tugra” does not apply specific trust limitations to its certificates in this policy.

Limitations to use (signature, website) for each type of certificate may be consulted in the previous section.

“e-tugra”, acting as provider of trust services, keeps internal records or ensures secure archiving of the following elements:

- 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

- 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”.

Pursuant to the “Regulation” and applicable legislation, the records pertaining to “QECs” laid down above 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 above must be kept for a period of not less than 10 years.

5. Subscriber Obligations

- Provide “e-tugra” with complete and appropriate information in accordance with the requirements described in the Certification Practice Statement, particularly with regard to the registration procedure.
- Guarantee that the information that should be included therein, is truthful, complete and up-to-date.
- Understand and accept the terms and conditions of use of the certificate, and any changes that may be made to the terms and conditions.
- Give prior consent to the issuance and delivery of a certificate.
- Guarantee proper use and conservation of certificate supports.
- Appropriately use the certificate, and specifically, comply with limitations to certificate use.
- Be diligent in custody of credentials, in order to prevent unauthorised uses, as established in the Certification Practises Statement.
- Notify “e-tugra” and any other individual that the subscriber believes may trust the certificate, without unjustifiable delays, of:
- The loss, theft of potential compromise of its credentials.
- Inaccuracy or changes to the certificate content, as notified to or suspected by the subscriber, calling for the revocation of the certificate when such changes constitute a cause for revocation.
- To stop using the identification means after the validity period has expired.
- Transfer specific obligations to key holders.
- Not monitor, manipulate or perform reverse engineering on technical implementation of certification services, without prior written authorisation from the Certification Entity.
- Not intentionally compromise the security of certification services.
- Will refrain from using the private keys corresponding to the public keys included in the certificates for the purpose of signing a certificate as if performing the function of a Certification Authority.

6. Certificate status checking obligations of relying parties

The following statements must be considered and complied with by any Relying Party:

- Receive notice and adhere to the conditions of the applicable CP and of the “e-tugra” CPS and associated conditions for Relying Parties.
- Decision to rely on a certificate must always be a conscious one and can only be taken by the Relying Party itself based on RFC 5280.
- Therefore, before deciding to rely on a certificate, one must be assured of its validity. If the Relying Party is not certain that its software performs such checks automatically, the Relying Party has to open the Certificate by clicking on it and checking that the Certificate **is NOT** either
    - **Expired**: by looking at the “valid from” and “valid to” notice; or
    - **Suspended or revoked:** by following the link to the Certificate Revocation List (CRL) and making sure that the certificate is not listed there, using the OCSP validation services.
- Never rely on expired or revoked certificates.
- Without prejudice to the warranties provided in the present CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it. “e-tugra” acting as ECSP accepts liability up to an aggregate limit as specified in the general terms and conditions for the concerned service for direct losses, due to non-compliance with this “e-tugra” CPS, towards a Relying Party reasonably relying on a Certificate.
- Without prejudice to the warranties provided in the applicable CP or in the “e-tugra” CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it.
- If a Relying Party relies on a Certificate without following the above rules, “e-tugra” will not accept liability for any consequences.
- The Relying Party is strongly advised not to rely upon the Information contained within their client application in use (browser) as to the usage of the Certificate and to check it against the Certificate Policy if in doubt.
- If a Relying Party becomes aware of or suspects that a Private Key has been compromised it will immediately notify “e-tugra” acting as ECSP.

Relying Parties must use online resources that the CA makes available through its repository to check the status of a Certificate before relying on it. “e-tugra” updates OCSP and CRLs at the following URLs:

- CRLs are available from http://crl.e-tugra.com
- OCSP service is available from http://ocsp.e-tugra.com/status/ocsp

7 Liability Limitation

"e-tugra" shall be held liable for,

- Harm and damage caused to any individual or entity, due to a lack of or delay in inclusion in the consulting service for the validity of certificates or expiry of certificate validity.
- Harm and damage caused to any individual, due to a lack of or delay in inclusion in the verification service for the validity of the identification mechanism.

- Additionally, "e-tugra" shall assume full liability for the actions of persons to which it has delegated authority to perform the functions necessary for rendering certification services.

“e-tugra” shall be held responsible for negligence or lack of due diligence in certification services provided, as well as when it fails to comply with obligations stipulated in legislation on electronic signatures.

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

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

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

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

8 Applicable Aggrements, CPS and CP

All applicable agreements, CP and CPS policies are available at https://www.e-tugra.com

9 Privacy Policy

9.1 Information treated as private

Registration Authorities undergo personal information processing during the identification and validation procedure of the Applicant which is treated as private. Personal information is not disclosed unless it is required by law or included in the certificate public information (for example the subject field of the certificate) with Applicant’s consent. If the Applicant agrees to include personal information related to personal identification described in CP/CPS related sections, in the Subscriber Certificate, then this information is not considered private.

9.2 Information not deemed private

Information included in the issued digital certificates is not considered private. If the Applicant, during the Certificate request process, requested personal information to be embedded in the issued Certificate, the Subscriber consents to “e-tugra”s disclosure of this information publicly by embedding the information in the issued Certificate. Subscriber Certificates are publicly disclosed at “e-tugra”s Repository, which implements restrictions to protect against enumeration attacks.

9.3 Responsibility to protect private information

All private and personal information handled and processed by “e-tugra”, is in accordance to the Turkish legislation concerning personal data protection. There are specific technical and organizational measures in place to prevent unauthorized and unlawful processing or accidental loss of private and personal information.

9.4 Information disclosure to judicial agencies

All non-classified information stored at the Certification and Registration Authorities is available to the law enforcement authorities, after their official written request. Classified and personal information can be disclosed to the judicial authority if there is an official court order according to the privacy and data protection applicable law. The process is carried out through the Information Security Board of “e-tugra”.

10. 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.

11. Applicable law, complaints and dispute resolution:

“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.

Dispute Resolution

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 Courts on Turkey shall have jurisdiction for the resolution of disputes.

12 Audits, Certifications And Repositories

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.

In order to develop and effectively implement these services, "e-tugra" has established an information security system for processes related to trust services, per standard ISO 27001.

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 3019 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.

A summary of these reports is also available at https://www.e-tugra.com