**Bugzilla ID:** 877744

**Bugzilla Summary:**

**General information about the CA’s associated organization**

|  |  |
| --- | --- |
| CA Company Name | E-Tugra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-TUGRA)(E-Tugra EBG Information Technologies and Services Corp.) |
| Website URL | [www.e-tugra.com.tr](http://www.e-tugra.com.tr) [www.e-tugra.com](http://www.e-tugra.com)  |
| Organizational type | E-Tugra is a Privately owned Organization, issuing certificates to the Public. E-Tugra is also a member of CA/Browser Forum |
| Primary Market / Customer Base | E-Tugra is a commercial CA with worldwide operations and customer base.E-Tugra is a privately held CA operating in Ankara, Turkey, with customers from all geographic areas within Turkey. E-TUGRA has been certified as one of the four authorized CAs that issues qualified certificates as well as SSL and code signing of certificates to public in Turkey. |
| Impact to Mozilla Users | Firefox users may encounter SSL certs that chain up to some of these roots |
| Inclusion in other major browsers | Existing root is included in Mozilla, NSS, Microsoft, Apple, Android, cs. For this root, inclusion processes are started for other browsers with Mozilla. |
| CA Contact Information | CA Email Alias: dtokgoz@symantec.comCA Phone Number: Davut Tokgoz, +90 532 430 66 34Title / Department: General Manager |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | E-Tugra Certification Authority |
| Certificate Issuer Field | CN = E-Tugra Certification AuthorityOU = E-Tugra Sertifikasyon MerkeziO = E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.L = AnkaraC = TR |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every 6 mounts (or as needed), and OCSP certificates. E-Tugra has other root certificates currently included in NSS. This root stands in a horizontal hierarchy with others.  |
| Root Cert URL | <http://www.e-tugra.com.tr/crt/>[Etugra\_Root.crt](http://www.e-tugra.com.tr/crt/Etugra_Root.crt) |
| SHA1 Fingerprint | ‎51 c6 e7 08 49 06 6e f3 92 d4 5c a0 0d 6d a3 62 8f c3 52 39 |
| Valid From  | 2013-03-05 |
| Valid To  | 2023-03-03 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA256WithRSA |
| Signing key parameters | 4096 bit |
| Test Website URL (SSL)Example Certificate (non-SSL) | <https://sslev.e-tugra.com.tr><https://sslov.e-tugra.com.tr> <https://ssldv.e-tugra.com.tr> |
| CRL URL | Root CA CRL URL:<http://crl.e-tugra.com/etugra_root.crl> DV SSL CRL URL:<http://crl.e-tugra.com/etugra_ssldv.crl>OV SSL CRL URL:<http://crl.e-tugra.com/etugra_sslov.crl>EV SSL CRL URL:<http://crl.e-tugra.com/etugra_sslev.crl>CPS 2.3. Time or Frequency of PublicationCRLs for subCAs are published every 6 (six) hours, 4 (four) times a day and with a validity time of 24 (twenty four) hours.  |
| OCSP URL | URL:<http://ocsp.e-tugra.com/status/ocsp> E-Tuğra provides uninterrupted on-line certificate status protocol OCSP supportSince we are always sending the current status in the OCSP response (never cached) we are not providing an expiration time in the response (no nextUpdate).  |
| Requested Trust Bits | Websites (SSL/TLS)Code Signing |
| SSL Validation Type | DV, OV, and EV |
| EV Policy OID(s) | 2.16.792.3.0.4.1.1.4EV Test result is attached to the bug. |
| Non sequential serial numbers and entropy in cert |  |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Root will be used to issue internally-operated SubCAs which will issue CodeSigning, SSL, and TimeStamping certificates and is offline.The subCAs are: * “E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı v2” -- Issues Qualified Certificates <http://www.e-tugra.com/crt/Etugra_NES_v2.crt>
* “E-Tugra Domain Validated CA” -- Issues DV SSL Certificates <http://www.e-tugra.com/crt/Etugra_SSLDV.crt>
* “E-Tugra Organization Validated CA” -- Issues OV SSL Certificates [http://www.e-tugra.com/crt/Etugra\_SSLDV.crt](http://www.e-tugra.com/crt/Etugra_SSLDV.crt%20)
* “E-Tugra Organization Validated CA” -- Issues EV SSL Certificates [http://www.e-tugra.com/crt/Etugra\_SSLDV.crt](http://www.e-tugra.com/crt/Etugra_SSLDV.crt%20)
 |
| Externally Operated SubCAs | None. E-Tugra roots do not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | None. None planned. No third parties can issue certificates signed by any E-Tugra roots. |
| Technical Constraints on Third-party Issuers | None. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | Language(s) that the documents are in: English and TurkishRepository: <http://www.e-tugra.com.tr/CPS> English CPS direct URL : <http://www.e-tugra.com.tr/Portals/3/engdoc/E-Tugra_SUE_v3.0_8_EN.pdf> English CP direct URL : <http://www.e-tugra.com.tr/Portals/3/engdoc/E-Tugra_SI_v3.0_8_EN.pdf>  |
| Audits | Audit Type: ETSI TS 101 456 Auditor: Turkish Information and Communication Technologies Authority (ICTA) Auditor Website: <http://www.btk.gov.tr/bilgi_teknolojileri/elektronik_imza/eshs.php> Audit Report: <http://www.btk.gov.tr/bilgi_teknolojileri/elektronik_imza/etura9.pdf> (2011.10.17) Audit Type: ETSI TS 102 042 - SSL NCP & EV-CP Auditor: BSI Group The Netherlands B.V. Auditor Website: http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search/Audit Report: will be informed when ready (we will have the audit statement on beginning of the August) |
| Baseline Requirements (SSL) | Since April, 2012, E-Tugra has issued certificates in full compliance with the CAB Forum Baseline Requirements.As per the CAB Forum Baseline Requirement # 8.3, where is the “Commitment to Comply” statement that should be in your CP or CPS? In Section 1, Introduction, of the CPS. |
| SSL Verification Procedures | *Information requested in #3 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA%3AInformation_checklist#Verification_Policies_and_Practices)* *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.*
	+ See <http://www.e-tugra.com.tr/cps> Section 3.2Initial Identity Validation
* If a challenge-response mechanism via email is used to confirm the ownership/control of the domain name, then provide the list of email addresses that are used for verification.
	+ See <http://www.e-tugra.com.tr/cps> Section 3.2.5. This list includes “admin‟, “administrator‟, “webmaster‟, “hostmaster‟, and “postmaster‟.
* *Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).* We confirm that we have such automatic blocks in place.
	+ *Specify the procedure for additional verification of a certificate request that is blocked*. If our automatic check detects a high-profile domain name, it flags the order for manual review. A trained Verification Specialist must review the application details and clear the flag if the order is legitimate. Another Verification Specialist will also review the these applications for cross control.
* *If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.*
	+ See <http://www.e-tugra.com.tr/cps> Section 3.2.2Authentication of Organization Identity
* If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.
	+ See <http://www.e-tugra.com.tr/cps> Section 3.2. There are special internal procedure how EV verification will be performed based on EV Guidelines on CabForum.
 |
| Organization Verification Procedures | See <http://www.e-tugra.com.tr/cps> Section 3.2.2Authentication of Organization Identity There are special internal procedure how EV verification will be performed based on Baselines Requirements on CabForum. |
| Email Address Verification Procedures | N/A |
| Code Signing Subscriber Verification Procedures | *Information requested in #5 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA%3AInformation_checklist#Verification_Policies_and_Practices)* *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the certificate subscriber's identity and authority, and the organization's identity and existence.*
	+ See <http://www.e-tugra.com.tr/cps> Section 3.2.2Authentication of Organization Identity
 |
| Multi-factor Authentication | *Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance or specify the technical controls that are implemented by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.* * *For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password?*

Yes.* *Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.*

Smartcard with its PIN which issued from an internal CA.* *This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.*

This applies to all accounts that can cause the approval and/or issuance of end-entity certificates.* *If technical controls are used instead of multi-factor auth for any accounts, then specify what those* technical controls are.

No additional technical controls are used for those accounts. E-Tugra complies with CabForum Requirements for System Security. And also see <http://www.e-tugra.com.tr/cps> Section 6.5. Computer Security Controls. |
| Network Security | E-Tugra maintains the own networks and systems with guidance of “[Network and Certificate System Security Requirements](https://www.cabforum.org/documents.html)” of Cab Forum.We confirm that we have done the above, and continue to do them on a regular basis.* Maintaining network security controls that at minimum meet the [Network and Certificate System Security Requirements.](https://www.cabforum.org/documents.html)
* Checking for mis-issuance of certificates, especially high-profile domains.
* Reviewing network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.
* Ensuring Intrusion Detection System and other monitoring software is up-to-date.
* Enable to shut down certificate issuance quickly if you are alerted of intrusion.
 |

**Response to Mozilla's CA Recommended Practices** ([https://wiki.mozilla.org/CA:Recommended\_Practices](https://wiki.mozilla.org/CA%3ARecommended_Practices))

|  |  |
| --- | --- |
| [Publicly Available CP and CPS](https://wiki.mozilla.org/CA%3ARecommended_Practices#Publicly_Available_CP_and_CPS) | See **Verification Policies and Practices**: Policy Documentation |
| [CA Hierarchy](https://wiki.mozilla.org/CA%3ARecommended_Practices#CA_Hierarchy) | See **Verification Policies and Practices**: CA Hierarchy  |
| [Audit Criteria](https://wiki.mozilla.org/CA%3ARecommended_Practices#Audit_Criteria) | See **Verification Policies and Practices:** Audits |
| [Document Handling of IDNs in CP/CPS](https://wiki.mozilla.org/CA%3ARecommended_Practices#Document_Handling_of_IDNs_in_CP.2FCPS) | E-Tugra participates in the Cab Forum, which has recently debated standards for IDN certificates. We intend to fully comply with whatever standards are drafted by that body.E-Tugra automated domain ownership process uses various ‘WHOIS” services to find the owner of a domain. We sure that in most cases of homographic spoofing, that automated process will fail, resulting in the order being flagged for manual review. Our verification specialists who perform manual review are trained to reject any domain name made up of multiple scripts. |
| [Revocation of Compromised Certificates](https://wiki.mozilla.org/CA%3ARecommended_Practices#Revocation_of_Compromised_Certificates) | See <http://www.e-tugra.com.tr/cps> Section 4.9 Certificate Revocation and Suspension. |
| [Verifying Domain Name Ownership](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Domain_Name_Ownership) | See <http://www.e-tugra.com.tr/cps> Section 3.2.2Authentication of Organization Identity |
| [Verifying Email Address Control](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Email_Address_Control) | N/A |
| [Verifying Identity of Code Signing Certificate Subscriber](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber) | See <http://www.e-tugra.com.tr/cps> Section 3.2.2Authentication of Organization Identity |
| [DNS names go in SAN](https://wiki.mozilla.org/CA%3ARecommended_Practices#DNS_names_go_in_SAN) | See <http://www.e-tugra.com.tr/cps> Section 3.1.5, 7.1.2, 7.1.4  |
| [Domain owned by a Natural Person](https://wiki.mozilla.org/CA%3ARecommended_Practices#Domain_owned_by_a_Natural_Person) | E-Tugra applies naming according to Section 9.2.4 Subject Distinguished Name Fields of the CAB Forum Baseline Requirements which E-Tugra complies with the latest version of it.  |
| [OCSP](https://wiki.mozilla.org/CA%3ARecommended_Practices#OCSP) | E-Tugra provides OCSP support for all certificates. OCSP service is updated online when certificate issued and or changed its status. |

**Response to Mozilla's list of Potentially Problematic Practices** ([https://wiki.mozilla.org/CA:Problematic\_Practices](https://wiki.mozilla.org/CA%3AProblematic_Practices))

|  |  |
| --- | --- |
| [Long-lived DV certificates](https://wiki.mozilla.org/CA%3AProblematic_Practices#Long-lived_DV_certificates) | E-Tugra complies with section 6 of the Mozilla CA Certificate Inclusion Policy. E-Tugra does not issue DV SSL more than 39 months. (CPS 6.3.2) |
| [Wildcard DV SSL certificates](https://wiki.mozilla.org/CA%3AProblematic_Practices#Wildcard_DV_SSL_certificates) | E-Tugra does not issue wildcard DV SSL. (CPS 3.1.5 and CPS 6.3.2) |
| [Email Address Prefixes for DV Certs](https://wiki.mozilla.org/CA%3AProblematic_Practices#Email_Address_Prefixes_for_DV_Certs) | When using the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, E-Tugra uses a mail system address formed in one of the following ways:* Taken from the Domain Name Registrant‟s “registrant”, “technical”, or “administrative” contact information, as it appears in the Domain‟s WHOIS record; or;
* By pre-pending a local part to a Domain Name as: webmaster@<domain\_name>, postmaster@<domain\_name>, admin@<domain\_name>, administrator@<domain\_name>, hostmaster@<domain\_name>.
 |
| [Delegation of Domain / Email validation to third parties](https://wiki.mozilla.org/CA%3AProblematic_Practices#Delegation_of_Domain_.2F_Email_validation_to_third_parties) | See <http://www.thawte.com/cps/index.html> Section 1.3.2 Registration Authorities and section 9.6.2. Registration Authority Responsibilities.E-Tugra does not delegate the RA functions for SSL (all for DV, OV, and EV) and Code Signing Certificates. |
| [Issuing end entity certificates directly from roots](https://wiki.mozilla.org/CA%3AProblematic_Practices#Issuing_end_entity_certificates_directly_from_roots) | None. E-Tugra issues certificates through subordinate CAs |
| [Allowing external entities to operate subordinate CAs](https://wiki.mozilla.org/CA%3AProblematic_Practices#Allowing_external_entities_to_operate_subordinate_CAs) | E-Tugra does not allow any external entities to operate subordinate CAs signed by any E-Tugra root. |
| [Distributing generated private keys in PKCS#12 files](https://wiki.mozilla.org/CA%3AProblematic_Practices#Distributing_generated_private_keys_in_PKCS.2312_files) | E-Tugra does not engage in this problematic practice. |
| [Certificates referencing hostnames or private IP addresses](https://wiki.mozilla.org/CA%3AProblematic_Practices#Certificates_referencing_hostnames_or_private_IP_addresses) | None. E-Tugra does not issue certificates for IP addresses and hostnames. |
| [Issuing SSL Certificates for Internal Domains](https://wiki.mozilla.org/CA%3AProblematic_Practices#Issuing_SSL_Certificates_for_Internal_Domains) | None. E-Tugra does not issue certificates for Internal Domains. For all SSL types, domain names are controlled via WHOSIS records and verified by the domain owner. |
| [OCSP Responses signed by a certificate under a different root](https://wiki.mozilla.org/CA%3AProblematic_Practices#OCSP_Responses_signed_by_a_certificate_under_a_different_root) | None. E-Tugra does not sign OCSP responses under a different root. |
| [CRL with critical CIDP Extension](https://wiki.mozilla.org/CA%3AProblematic_Practices#CRL_with_critical_CIDP_Extension) | None. E-Tugra issues only “full” CRLs and does not use partitioned CRLs |
| Generic names for CAs | E-Tugra root and subordinate CA uses meaningful names approximate to usage of the Certificates and CA name includes the company name |
| Lack of Communication With End Users | E-Tugra contact information is available based on 24 hours 7 days and has dedicated procedures for complaints which was handled agents based 7 days and 12 hours. |

}