Bugzilla ID: 877744
Bugzilla Summary: Adding E-Tuğra EBG new root certificate in Mozilla and enable it for EV

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
   a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
   b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

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 www.e-tugra.com
Organizational type	E-Tugra is a Privately owned Organization, issuing certificates to the Public.
Primark 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.
Inclusion in other major browsers	Existing root is included in Mozilla (NSS), Microsoft, Apple, Android.
CA Contact Information	CA Email Alias: dtokgoz@symantec.com CA Phone Number: Davut Tokgoz, +90 532 430 66 34 Title / Department: General Manager

Technical information about each root certificate

Certificate Name	E-Tugra Certification Authority

Certificate Issuer Field	CN = E-Tugra Certification Authority
	OU = E-Tugra Sertifikasyon Merkezi
	O = E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
	L = Ankara
	C = TR

Certificate Summary	This SHA-256 root will eventually replace the "EBG Elektronik Sertifika Hizmet Sağlayıcısı" root that was included via Bugzilla Bug #443653. This root signs internally-operated subordinate CAs that issue certificates for SSL, Code Signing, and Timestamping.
Root Cert URL	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	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096

Test Website URL	https://sslev.e-tugra.com.tr -- error: Firefox can't find the server at sslev.e-tugra.com.tr. https://sslov.e-tugra.com.tr -- error: Firefox can't establish a connection to the server at sslov.e-tugra.com.tr. https://ssldv.e-tugra.com.tr -- Firefox can't find the server at 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 (NextUpdate: 24 hours) OV SSL CRL URL: http://crl.e-tugra.com/etugra_sslov.crl (NextUpdate: 24 hours) EV SSL CRL URL: http://crl.e-tugra.com/etugra_sslev.crl (NextUpdate: 24 hours) CPS 2.3: CRLs 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	http://ocsp.e-tugra.com/status/ocsp What is the maximum expiration time that is set in the OCSP responses?
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type	DV, OV, and EV
EV Policy OID(s)	2.16.792.3.0.4.1.1.4 Please test EV, and attach a screenshot to the bug that shows the EV treatment. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Let me know if you need help creating the test_ev_roots.txt file, or if you run into problems with the testing, after you've made sure the test website, CA hierarchy, and OCSP are all working as per https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version#Not_Getting_EV_Treatment.3F

CA Hierarchy information for each root certificate

CA Hierarchy	This (offline) root will be used to issue internally-operated SubCAs which will issue CodeSigning, SSL, and TimeStamping certificates. The subCA certs (listed below) may be downloaded from http://www.e-tugra.com/crt/ - "E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı v2" -- Issues Qualified Certificates - "E-Tugra Domain Validated CA" -- Issues DV SSL Certificates - "E-Tugra Organization Validated CA" -- Issues OV SSL - "E-Tugra Organization Validated CA" -- Issues EV SSL Certificates
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	Not applicable.

Verification Policies and Practices

Policy Documentation	Documents are in English and Turkish Repository: http://www.e-tugra.com.tr/CPS CPS (English): http://www.e-tugra.com.tr/Portals/3/engdoc/E-Tugra_SUE_v3.0_8_EN.pdf CP (English): 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. **When do you expect to have the current audit statement?**
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, the “Commitment to Comply” statement is in Section 1, Introduction, of the CPS.
Organization Verification Procedures	CPS Section 3.2.2 summarizes the authentication of organization identity for premium SSL and CSC (code signing) certs, and EV SSL and EV CSC certs. Standard SSL certs are DV, so no verification of legal identity. There are special internally-documented procedures how EV verification will be performed.
SSL Verification Procedures	CPS Section 3.2.5: 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. CPS Section 4.1.2: 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.
Email Address Verification Procedures	Not applicable. Not requesting the email trust bit.

Code Signing Subscriber Verification Procedures	CPS Section 3.2.2 Authentication of Organization Identity CPS Section 4.1.2: 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 applicationapproval. 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.
Multi-factor Authentication	Smartcard with its PIN which issued from an internal CA. This applies to all accounts that can cause the approval and/or issuance of end-entity certificates. E-Tugra complies with CabForum Requirements for System Security. 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” of Cab Forum. CPS Sections 5 and 6.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
Document Handling of IDNs in CP/CPS	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	CPS Section 4.9
Verifying Domain Name Ownership	Yes. See above.
Verifying Email Address Control	Not applicable.
Verifying Identity of Code Signing Certificate Subscriber	Yes. See above.
DNS names go in SAN	CPS Section 7.1.2.2: Subject Alternative Name: (is optional) May contain alternative domain names of the subject on server. **I don’t think this complies with Baseline Requirement #9.2.1.**
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	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)

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	E-Tugra does not issue wildcard DV SSL. (CPS 3.1.5 and CPS 6.3.2)
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	E-Tugra does not delegate the RA functions for SSL and Code Signing Certificates. (CPS sections 1.3.2 and 9.6.2)
Issuing end entity certificates directly from roots	No. See above.
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	CPS section 4.1.2: The generation of public and private key is done by the applicant.
Certificates referencing hostnames or private IP addresses	E-Tugra does not issue certificates for IP addresses and hostnames.
Issuing SSL Certificates for Internal Domains	E-Tugra does not issue certificates for Internal Domains.
OCSP Responses signed by a certificate under a different root	Needs to be tested. See above.
CRL with critical CIDP Extension	CRLs imported without error into Firefox.
Generic names for CAs	Root and subCA certs have CNs containing E-Tugra.
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.