Bugzilla ID: 443653
Bugzilla Summary: Add Root (EBG Informatic Technologies and Services Corp. (E-Tugra))

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-TUGRA)
Website URL	http://etugra.com.tr (in Turkish)
Organizational type	Private Corporation
Primary market / customer base	E-TUGRA is the EBG Informatics Technologies and Services Corporation. 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 other types of certificates to public in Turkey.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	EBG Elektronik Sertifika Hizmet Sağlayıcısı
Cert summary / comments	From this root CA E-TUGRA has issued two internally-operated subordinate CAs. The Qualified Certificate (QC) subordinate CA issues certificates for Digital Signing and Non-Repudiation (document and email signing). The Non Qualified Certificate (NQC) subordinate CA (EBG Web Sunucu Sertifika Hizmet Sağlayıcısı) issues certificates for SSL, email encryption, and code signing.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=380381
SHA-1 fingerprint.	8c:96:ba:eb:dd:2b:07:07:48:ee:30:32:66:a0:f3:98:6e:7c:ae:58
Valid from	2006-07-17
Valid to	2016-08-14
Cert Version	3
Modulus length	4096
Test Website	https://webmail.takasbank.com.tr/
CRL	http://crl.e-tugra.com.tr/e-tugra_ksm.crl http://crl.e-tugra.com/e-tugra_asm_ssl.crl NextUpdate: 24 hours CPS Section 4.9.7: "CRL's are published every 24 hours."

OCSP	http://ocsp.e-tugra.com/status/ocsp CPS: 4.10.2 Service Accessibility E-TUGRA provides CRL and OCSP services non-stop on the basis of 24 hours in 7 days. In case CRL and OCSP services are interrupted beyond E-TUGRA control, ETUGRA does its best to ensure resumption of the services within maximum 24 hours.
List or description of subordinate CAs operated by the CA organization associated with the root CA.	From this root CA E-TUGRA has issued two internally-operated subordinate CAs. The Qualified Certificate subordinate CA issues certificates for Digital Signing and Non-Repudiation (document and email signing). The NQC subordinate CA (EBG Web Sunucu Sertifika Hizmet Sağlayıcısı) issues certificates for SSL, email encryption, and code signing.
subordinate CAs operated by third parties	There are no subordinate CAs that are operated by third parties.
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV – All end-entity SSL certs are both Domain Validated and Identity/Organizationally validated.
EV policy OID	Not EV
CP/CPS	Non Qualified (NQC) CP/CPS in English: http://www.e-tugra.com.tr/Portals/3/Templates/NQC_CpCps.pdf This CPS applies to NQC's for Server Authentication (SSL Server), NQC's for Code Signing, and for email. Qualified CP/CPS in English: http://www.e-tugra.com.tr/Portals/3/Templates/QC_CpCps.pdf
AUDIT	Audit Type: ETSI 101 456 Auditor: Turkish Information and Communications Technologies Authority (ICTA) Auditor Website URL: http://www.tk.gov.tr Audit Document URL(s): http://www.e-tugra.com.tr/Portals/3/E-Tugra_audit_09.pdf (2008.05.30) <http://www.tk.gov.tr/eimza/eshs.htm> has links to Turkish government information relating to the CA.

	> Subject: RE: Requesting Confirmation of Authenticity of Audit Statement for E-Tugra > As one of the audit team members I would like to confirm that we (ICTA) have issued the audit statement at the > mentioned URL. > In Turkey, electronic certificate service provider such as e-Tugra shall be inspected by the ICTA when it is > necessary and at least biannual at the ICTA's own initiative. > Yours sincerely > Demet KABASAKAL > Information Technologies and Communication Authority

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - NQC CP/CPS Section called Validation of the Domain Names of the Natural Persons and Legal Entities:
        - In the case of individual and corporate applications, if the application is for a Secure Web Server Certificate, the domain name for the application is verified. The verification is achieved via web based query. The Turkish domains which ends with .tr extension are queried from the Turkish domain names legal registrar address https://www.nic.tr/. In case the domain is a foreign domain, then the query is made via international sites such as http://www.domaintools.com/ or http://whois.mtgsy.net/default.php
- Verify the email account associated with the email address in the cert is owned by the subscriber.
    - NQC CP/CPS Section called Verification of the e-mail addresses of the Natural Persons and Legal Entities:
        - In the case of individual and corporate applications, if the application includes e-mail protection then the e-mail address of the applicant is verified by means of an e-mail authentication and a secret question challenge. This is done by sending an e-mail to the proclaimed e-mail address which includes a challenge question which is already obtained from the NQC application form. In case a reply from the applicants proclaimed e-mail address is received and the answer to the challenge question is correct, then the verification process is successfully completed. The application failing from either of the two challenges described above is denied.
- Verify identity info in code signing certs is that of subscriber
    - NQC CP/CPS Section called Verification of the ID's of the Natural Persons:
        - In the case of individual and corporate applications, the ID of a natural person is verified by means of face to face Authentication based on at least two photographed and valid documents such as ID cards, passports and driving licenses. In the case of corporate applications, it is not obligatory to conduct face to face Authentication.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates

    - SSL certs are OV
- Wildcard DV SSL certificates
    - SSL certs are OV
- Delegation of Domain / Email validation to third parties
    - No.
- Issuing end entity certificates directly from roots
    - No. End entity certs are issued through the subordinate CAs.
- Allowing external entities to operate unconstrained subordinate CAs
    - No. The two subordinate CAs are operated internally.
- Distributing generated private keys in PKCS#12 files
    - Not Found
- Certificates referencing hostnames or private IP addresses
    - Not Found
- OCSP Responses signed by a certificate under a different root
    - Test site loads without error into Firefox when OCSP is enforced.
- CRL with critical CIDP Extension
    - CRLs imported into Firefox without error
- Generic names for CAs
    - CA name is not generic

Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
    - Posted on the Turkish Telecommunications Agency website
    - Confirmed authenticity of the letter from the auditor that states ETSI 101 456 compliance.
- For EV CA's, verify current WebTrust EV Audit done.
    - Not Applicable
- Review Audit to flag any issues noted in the report
    - No issues noted