Bugzilla ID: 433845
Bugzilla Summary: Add TÜRKTRUST Root CA

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	TÜRKTRUST
Website URL	http://www.turktrust.com.tr/ English: http://www.turktrust.com.tr/ingilizce/homepage.jsp
Organizational type	Public Corporation
Primary market / customer base	TÜRKTRUST Information Security Services Inc. is an IT company based in Turkey. TÜRKTRUST is an authorized qualified electronic certificate service provider according to the Turkish Electronic Signature Law. TÜRKTRUST issues qualified certificates, time-stamping services, SSL certificates, and object signing certificates.
CA Contact Information	Email Alias: sertifika@turktrust.com.tr Phone Number: 90-312-439-1000 Title/Department: Certificate Services

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

Info Needed	**Data**
Certificate Name	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı

Issuer	O = TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Aralık 2007
	CN = TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
	L = Ankara
	C = TR

Cert summary / comments	This is an offline root with internally-operated subordinate CAs that sign end-entity certificates. TÜRKTRUST has other root certificates currently included in NSS. This root stands in a horizontal hierarchy with others.
Root Cert URL	http://www.turktrust.com.tr/sertifikalar/TURKTRUST_Elektronik_Sertifika_Hizmet_Saglayicisi_s3.crt
SHA-1 fingerprint	F1:7F:6F:B6:31:DC:99:E3:A3:C8:7F:FE:1C:F1:81:10:88:D9:60:33
Valid from	2007-12-25
Valid to	2017-12-22
Cert Version	3
Modulus length / key length	2048
Test Website	https://evssl.turktrust.com.tr/ Need TURKTRUST to perform the EV testing as described here before I create the PSM bug. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version (this item will not hold up discussion, but will be needed before I can file the PSM bug)
CRL	http://www.turktrust.com.tr/sil/TURKTRUST_Kok_SIL_s3.crl http://www.turktrust.com.tr/sil/TURKTRUST_SSL_SIL_s3.crl http://www.turktrust.com.tr/sil/TURKTRUST_EV_SSL_H3_S2.crl CPS Section 4.10.1: TURKTRUST publishes CRL twice a day within 12 (twelve) hour intervals with a validity period of 24 (twentyfour) hours even if there is no change in the status of certificates.

OCSP	http://ocsp.turktrust.com.tr Section 4.9.9: TÜRKTRUST provides uninterrupted on-line certificate status protocol OCSP support.
CA Hierarchy	This is an offline root with internally-operated subordinate CAs which sign end-entity certificates. The subCAs are: 1) "TÜRKTRUST Nitelikli Elektronik Sertifika Hizmetleri" -- Issues Qualified Certificates http://www.turktrust.com.tr/sertifikalar/TURKTRUST_Nitelikli_Elektronik_Sertifika_Hizmetleri_s3.crt 2) "TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri"– Issues SSL Certificates 3) "TÜRKTRUST EV SSL Sunucu Sertifikası Hizmetleri H3 - Sürüm 2" – Issues EV SSL Certificates
Externally Operated SubCAs	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Code (Code Signing)
SSL Validation Type	OV and EV
EV policy OID(s)	2.16.792.3.0.3.1.1.5
CP/CPS	The documents are provided in Turkish and English. Document Repository: http://www.turktrust.com.tr/en/bilgideposu.html CP (English): http://www.turktrust.com.tr/en/files/bilgidepo/TURKTRUST_CP_V-05_%5BEN%5D_(01.11.2011).pdf CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=612540
AUDIT	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/TURKTRUST_LETTER_2011.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/ ETSI Certificate: https://bugzilla.mozilla.org/attachment.cgi?id=585759 (2011.12.20)
Organization Identity Verification	CPS Section 3.2.2 and 3.2.3.
Domain Name Ownership / Control	No automatic issuance. For SSL certificates issued to organizations, TÜRKTRUST validates the identity of the organization's representative and his or her authorization to request the certificate, and also verifies ownership of the associated domain. (See CPS sections 3.2 and 4.2) Non-EV: CPS Section 3.2.2.1: "The name of legal entity is verified against the official documents of the country of residence of the applicant. Verification herein is executed according to the TURKTRUST procedures. The e-mail address submitted by the authorized person who conducts the application operations on behalf of the subscriber should be verified. This verification is done with a unique user name and activation code sent to the authorized person's e-mail address." EV: CP and CPS Section 3.2.2.2
Email Address Ownership / Control	Not applicable. Not requesting the Email trust bit.

Identity of Code Signing Subscriber	Object Signing certificates are only issued to organizations, and not to individuals. For object signing certificates issued to organizations, TÜRKTRUST validates the identity of the organization's identity, the identity of the organization’s representative and their authorization to request the certificate. (See CPS sections 3.2 and 4.2)
Multi-factor Authentication	See CPS section 6.2.2, Private Key Multi-Person Control. As regards to the "segregation of duties" principle, seperate roles have been assigned to authorized personnel. Any certificate application is subject to manuel controls at different phases. At each access control level for certificate issuance, m-of-n multi factor authentication mechanisms including biometrics are mandatory. All domain names (irrespective of whether it be high or low profile) are manually processed and verified.
Network Security	See CPS sections 6.5, 6.6, and 6.7.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV and EV. o CPS section 6.3.2: The term for QECs, SSL certificates and OSCs issued by TURKTRUST is 1 (one), 2 (two) or 3 (three) year(s). … The term for EV SSL certificates issued by TURKTRUST is 1 (one), 2 (two) year(s) or at most 27 (twenty seven) months. • Wildcard DV SSL certificates o SSL certs are OV. o Wildcard certs are allowed for OV certs, not for EV certs. • Delegation of Domain / Email validation to third parties o External Registration Authorities may be used. o CPS 1.3.2: Actions associated with registration centers may be performed by registration units within the TURKTRUST center in response to certificate requests arriving from TURKTRUST sales representatives as well as by registration centers affiliated with TURKTRUST. In both cases, certificate requests are relayed to the TURKTRUST’s issuing certification authority and the certificates are issued. o CPS 9.6.2: Registration centers under TURKTRUST represent and warrant that identity validation have been performed accurately and reliably for the applicants according to the certificate types as stated in this CPS document, records are kept accurately, certificate issuing, renewal and revocation requests transmitted to the CA center have been accurate and complete. • Issuing end entity certificates directly from roots o Certs are issued through subordinate CAs • Allowing external entities to operate unconstrained subordinate CAs o All subordinate CAs are internally operated • Distributing generated private keys in PKCS#12 files o CPS section 6.2.8: Private keys of SSL, EV SSL and OSCs shall be activated on the software or hardware belonging to the subscriber. • Certificates referencing hostnames or private IP addresses o No • Issuing SSL Certificates for Internal Domains o No • OCSP Responses signed by a certificate under a different root

	○ No • CRL with critical CIDP Extension ○ No • Generic names for CAs ○ CA name includes the company name