Bugzilla ID: 433845
Bugzilla Summary: Add more TÜRKTRUST Root CAs

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
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. The main aim of this root is to issue certificates for Mobile PKI (i.e. mobile signatures).
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	Coming soon.
CRL	URI: http://www.turktrust.com.tr/sil/TURKTRUST_Kok_SIL_s3.crl End-Entity SSL cert CRL: http://www.turktrust.com.tr/sil/TURKTRUST_SSL_SIL_s3.crl (NextUpdate: 2 days) CPS Section 4.9.7: Certificate Revocation Lists (CRL) Issuance Frequency TÜRKTRUST issues a new CRL at least once a day even if there is no change in the status of end user 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

Externally Operated SubCAs	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code (Code Signing)
SSL Validation Type DV, OV, and/or EV	IV/OV
EV policy OID(s)	Not requesting EV at this time
CP/CPS	CPS (English): http://www.turktrust.com.tr/pdf/cps_third.pdf
AUDIT	Audit Type: ETSI TS 101 456 Auditor: Republic of Turkey Information and Communication Technologies Authority (ICTA) Auditor Website: http://www.btk.gov.tr Audit Statement: http://www.btk.gov.tr/bilgi_teknolojileri/elektronik_imza/eshs.php (2010.05.02)
Organization Identity Verification	CPS Section 3.2.2: When issuing certificates for servers belonging to companies or institutions or for individual applicants who will obtain certificates on behalf of companies or institutions, the commercial titles of companies or the official names of institutions should be verified based on official documents. To verify company or institution information, the company's commercial register extract and the signature circular of company's authorized persons are required. CPS Section 3.2.3, Authentication of Individual Identity Personal information for persons applying for qualified electronic certificates should be verified in the way stated in the laws and based on official documents. When receiving the applications for qualified electronic certificates, authentication shall be made face to face at the first application pursuant to the law. For applications for trial certificates, a valid e-mail address and a personal statement suffice. To verify personal identity in applications for qualified electronic certificates, the originals of one of the official identity documents such as an identity certificate, a driver's license or a passport shall be shown and photocopies furnished. TÜRKTRUST shall confirm that the copies conform to the originals. In institutional applications for the employees of an institution, personal information for persons to be included in the certificate shall be verified in the way stated in the laws and based on official documents. When receiving applications for qualified electronic certificates, authentication shall be made face to face at the first application pursuant to the law. Further in institutional applications, the commercial register extract and other relevant documents shall be required to determine the legal personality of the institution. The e-mail addresses of people applied for qualified electronic signature are taken from personal declarations from the application form. To verify those addresses before to be added to the certificate, a unique (URL) link specific to the application is sent to the correspondent enclosed in an e-mail message. The e-mail address is verified by clicking to this URL and e-mail address can be added to the target certificate after that.
Domain Name Ownership / Control	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 3.2.2 and 4.2.1) From CPS Section 4.2.1: "When processing a server certificate application, the domain name that belongs to the server, the server's name and the name of the domain owner and personal information for the server administrator should be verified by TÜRKTRUST's registration authorities. The information published by authorized resources are used for the verification of the domain name ownership. (www.nic.tr records for domain names with ".tr" extension, international resources are based on for other domain names)"

Email Address Ownership / Control	For certificates issued to individuals, TÜRKTRUST verifies both identity and control of the email account associated with the email address referenced in the certificate. (See CPS Section 3.2.3) From CPS Section 3.2.3: "The e-mail addresses of people applied for qualified electronic signature are taken from personal declarations from the application form. To verify those addresses before to be added to the certificate, a unique (URL) link specific to the application is sent to the correspondent enclosed in an e-mail message. The e-mail address is verified by clicking to this URL and e-mail address can be added to the target certificate after that."
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 verifies the organizational identity as per CPS section 3.2.2. From CPS section 3.2.1: "The corporate names are used in object signing certificates which are validated according to formal documents."

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV.
	  ○ CPS Section 4.7: "For end user certificates, the same private and public key pay may be used for up to a maximum of 3 (three) years."
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV.
	  ○ Did not find anything indicating that wildcard certs were allowed.
	• Delegation of Domain / Email validation to third parties
	  ○
	• Issuing end entity certificates directly from roots
	  ○ Certs are issued through subordinate CAs
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ All subordinate CAs are internally operated
	• Distributing generated private keys in PKCS#12 files
	  ○
	• Certificates referencing hostnames or private IP addresses
	  ○ Not found
	• Issuing SSL Certificates for Internal Domains
	  ○ Not found
	• 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