Bugzilla ID: 1007683
Bugzilla Summary: Add TÜRKTRUST Root CA for TÜRKTRUST Root Hierarchy 5 and 6

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	TURKTRUST
Website URL	http://www.turktrust.com.tr/en
Organizational type	Private Corporation
Primark 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.
Impact to Mozilla Users	TURKTRUST issues certificates to the public. One of TURKTRUST's previously included root certs expires this November.
Inclusion in other major browsers	TURKTRUST has roots included in the stores of Mozilla, Microsoft, Opera, Apple (Safari), and Google (Android)
CA Primary Point of Contact (POC)	POC direct email: mert.ozarar@turktrust.com.tr Email Alias: sertifika@turktrust.com.tr CA Phone Number: 90-533-7764656 Title/Department: Technical Department

Technical information about each root certificate

Cert Name	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H6

Cert Issuer Field	CN = TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5
	O = TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
	L = Ankara
	C = TR
		CN = TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H6
		O = TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
		L = Ankara
		C = TR

Cert Summary	The H5 root has internally-operated subCAs that issue SSL and Code Signing certificates.	The H6 root has an internally-operated subCA that issues EV SSL certificates.
Root Cert URL	http://www.turktrust.com.tr/sertifikalar/TURKTRUST_Elektronik_Sertifika_Hizmet_Saglayicisi_h5.crt	http://www.turktrust.com.tr/sertifikalar/TURKTRUST_Elektronik_Sertifika_Hizmet_Saglayicisi_h6.crt
SHA1 Fingerprint	C4:18:F6:4D:46:D1:DF:00:3D:27:30:13:72:43:A9:12:11:C6:75:FB	8A:5C:8C:EE:A5:03:E6:05:56:BA:D8:1B:D4:F6:C9:B0:ED:E5:2F:E0
Valid From	2013-04-30	2013-12-18
Valid To	2023-04-28	2023-12-16

Cert Version	3	3
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	2048	2048
Test Website	https://testsuite12001.turktrust.com.tr Get error when OCSP-hard-fail set: Error code: sec_error_ocsp_server_error See: https://wiki.mozilla.org/CA:Recommended_Practices#OCSP	https://testsuite12002.turktrust.com.tr
CRL URL	http://www.turktrust.com.tr/sil/TURKTRUST_SSL_SIL_h5.crl http://www.turktrust.com.tr/sil/TURKTRUST_Kok_SIL_h5.crl	http://www.turktrust.com.tr/sil/TURKTRUST_EV_SSL_SIL_h6.crl http://www.turktrust.com.tr/sil/TURKTRUST_Kok_SIL_h6.crl
OCSP URL	http://ocsp.turktrust.com.tr	http://ocsp.turktrust.com.tr
Requested Trust Bits	Websites (SSL/TLS) Code Signing	Websites (SSL/TLS)
SSL Validation Type	DV, OV	EV
EV Policy OID	N/A	2.16.792.3.0.3.1.1.5
Non-sequential serial numbers, entropy in cert	Yes	Yes

CA Hierarchy information for each root certificate

CA Hierarchy	http://www.turktrust.com.tr/en/kok_sertifika_kurulumu2.html TURKTRUST ECSP 6. ROOT HIERARCHY Root: TURKTRUST Electronic Certificate Service Provider Certificate EV SSL subCA: TURKTRUST Electronic Server Certificate Services Certificate (EVSSL)	http://www.turktrust.com.tr/en/kok_sertifika_kurulumu2.html TURKTRUST ECSP 5. ROOT HIERARCHY Root: TURKTRUST Electronic Certificate Service Provider Certificate SSL subCA: TURKTRUST Electronic Server Certificate Services Certificate Non-QEC subCA: TURKTRUST Simple Electronic Certificate Services Certificate Code-Signing subCA: TURKTRUST Object Signing Services Certificate

Externally Operated SubCAs	None	None
Cross-Signing	None	None
Technical Constraints on Third-party Issuers	No third-party issuers.	No third-party issuers.

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: Turkish & English Document Repository: http://www.turktrust.com.tr/en/bilgideposu.html CP (EN): http://www.turktrust.com.tr/files/bilgidepo/TURKTRUST_CP_V-08_%5BEN%5D.pdf CPS (EN): http://www.turktrust.com.tr/files/bilgidepo/TURKTRUST_CPS_V-08_%5BEN%5D.pdf
Audits	Audit Type: ETSI TS 102 042 v2.4.1 – NCP, PTC-BR, EV-CP Auditor: BSI (http://www.bsigroup.com) ETSI Certificate: ETS 019 Audit Statement: http://www.turktrust.com.tr/en/images/page/hakkimizda/belgeler/big/etsinew1.png (2013.09.16) http://www.turktrust.com.tr/en/images/page/hakkimizda/belgeler/big/etsinew2.png
Baseline Requirements (SSL)	URL to BR audit statement: same as above CPS and CP section 1: "Moreover, for SSL and EV SSL certificates TURKTRUST conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document published at http://www.cabforum.org and referenced from the ETSI TS 102 042 standard."
Organization Verification Procedures	CPS section 3.2.2.1, QEC, SSL or OSC: For SSL and OSC applications, 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. CPS section 3.2.2.2, EV SSL: In verification of an EV SSL application, minimum criteria to be met are as follows: - The name of legal entity is verified against the official documents of the country of residence of the applicant. Additional to this verification, circular of signature or an equivalent official document in applicable legislation, showing the authority of the applicant to act on behalf of the legal entity is required. - Operational existence of the legal entity is confirmed via a third party, who is a buyer of a product or service of the legal entity. Where possible, an official document, obtained from a public agency or a legally authorized person to do so, proving the operational existence suffices to verify. - Address of the legal entity's place of business is verified according to the legal documents of the country of residence. Moreover, telephone numbers, submitted by the applicant, are checked if they are exactly matched with the official records. In case of mismatch, correction is required. Verified telephone is the called for applicant to confirm the application. - 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.

	- The following conditions should be met as well: -- The legal entity is the owner of the DNS registry, or -- The legal entity is given the exclusive right and authority to use the DNS name. All conditions that apply for authentication of legal entity for an EV SSL applicant are given in Appendix. Given the conditions here, the process of authentication of legal persons is conducted according to the TURKTRUST procedures. CPS section 3.2.5: In cases where the name of a legal entity is to be contained in a certificate, the applicant must submit an official document showing the authority of the applicant to act on behalf of the legal entity.
SSL Verification Procedures	CPS section 9.6.1, CA Representations and Warranties: - Right to Use Domain Name: TURKTRUST has taken all steps reasonably necessary to verify that, as of the date the SSL and EV SSL certificate was issued, either the Subject named in the SSL and EV SSL certificate has the exclusive right to use all the Domain Name(s) listed in the SSL and EV SSL certificate or had control of, the Domain Name(s) listed in the certificate's subject field and subjectAltName extension. This verification is done either communicating directly with the national or international domain name registrant or right to use domain name assignment. - Authorization for SSL and EV SSL Certificate: TURKTRUST has taken all steps reasonably necessary to verify that the Subject named in the SSL and EV SSL certificate has authorized the issuance of the SSL and EV SSL certificate. This authorization verification is done by either official authorization document or the data which is taken from independent resources and confirmed via telephone or it can be done face to face.
Email Address Verification Procedures	Not Applicable. Not requesting the Email trust bit.
Code Signing Subscriber Verification Procedures	CPS section 1.2: TURKTRUST OSC Policy (2.16.792.3.0.3.1.1.4) covers certificates related to object signing operations. OSC is issued and maintained in conformity with "Normalized Certificate Policy" defined in ETSI TS 102 042. CPS section 1.6.2: Object Signing Certificate (OSC): The certificate that verifies the owner of the source code of software that can be executed on a computer. CPS section 3.1.5.4. OSC: DN in TURKTRUST OSC is formed as below: - "CN" contains complete name of the subscriber, which is based on the official documentation according to the legislation of residence. CPS section 3.2.2.1. QEC, SSL or OSC 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. For SSL and OSC applications, 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. CPS section 4.1.1, Who Can Submit a Certificate Application? Any real person free of any legal obstacles may apply for QEC or OSC. For SSL, EV SSL and OSC, including private legal entities and public entities, any legal entity may apply for a certificate.

Multi-factor Authentication	We confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance.
Network Security	We confirm that we have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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

Publicly Available CP and CPS	See above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	Yes
Revocation of Compromised Certificates	Yes. CPS section 4.9.1
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	Yes CPS section 3.1.5.2: "SAN" contains the "DNS" which is indicated in "CN" field. Provided that domain name ownership is verified for each domain name, more than one domain name can be written in this field. The constraints which are specified in "CN" are also valid for SAN field.
Domain owned by a Natural Person	See above
OCSP	See above

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	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). For the sake of cryptographic security of the key pairs, the total validity period with the same content for QECs cannot exceed 3 years. 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	CPS section 3.1.5.2: In wildcard SSL certificates, CN field contains "*.<DNS name>". This field cannot contain "*.com" or "*.com.tr" which do not show the fully qualified domain name. o Wildcards are not issued for EV SSL certificates.
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	???
Issuing end entity certificates directly from roots	No. See above.
Allowing external entities to operate subordinate CAs	No. See above.

Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	CPS section 3.1.5.2: CN field cannot contain IP addresses or internal server names in SSL or EV SSL certificates.
Issuing SSL Certificates for Internal Domains	CPS section 3.1.5.2: CN field cannot contain IP addresses or internal server names in SSL or EV SSL certificates.
OCSP Responses signed by a certificate under a different root	See above
CRL with critical CIDP Extension	???
Generic names for CAs	See above
Lack of Communication With End Users	???
Backdating the notBefore date	???