Bugzilla ID: 715136
Bugzilla Summary: Add Renewed TURKTRUST root certificate

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	TÜRKTRUST
Website URL	http://www.turktrust.com.tr/
Organizational type	Public corporation
Primark Market / Customer Base	TÜRKTRUST is a commercial CA operating in the Republic of Turkey.
CA Contact Information	CA Email Alias: sertifika@turktrust.com.tr CA Phone Number: (90-312) 439 10 00 Title / Department:

Technical information about each root certificate

Certificate Name	Friendly name to be used when displaying information about the root. Usually the CN.
Certificate Issuer Field	The Organization Name and CN in the Issuer must have sufficient information about the CA Organization.
Certificate Summary	
Root Cert URL	
SHA1 Fingerprint	
Valid From	YYYY-MM-DD
Valid To	YYYY-MM-DD
Certificate Version	
Certificate Signature Algorithm	
Signing key parameters	RSA modulus length; e.g. 2048 or 4096 bits. Or ECC named curve, e.g. NIST Curve P-256, P-384, or P-512.
Test Website URL (SSL)	If requesting EV treatment, the test website cert should be an EV cert chaining up to this root.
CRL URL	URL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS. Test: Results of importing into Firefox browser
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Testing results a) Browsing to test website with OCSP enforced in Firefox browser b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	Websites (SSL/TLS)

	Email (S/MIME) Code Signing
SSL Validation Type	OV and EV
EV Policy OID	2.16.792.3.0.3.1.1.5

CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	The documents are provided in Turkish and English. Document Repository: http://www.turktrust.com.tr/en/bilgideposu.html CP: http://www.turktrust.com.tr/en/files/bilgidepo/TURKTRUST_CP_V-05_%5BEN%5D_(01.11.2011).pdf CPS: http://www.turktrust.com.tr/en/files/bilgidepo/TURKTRUST_CPS_V-05_%5BEN%5D_(01.11.2011).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/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)
SSL Verification Procedures	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
Organization Verification Procedures	CPS Section 3.2
Email Address Verification Procedures	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 3.2.2.1) CPS Section 3.2.2.1: "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."
Code Signing Subscriber Verification Procedures	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	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you 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	Yes
CA Hierarchy	?
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	CPS section 4.9.1, Circumstances for Revocation
Verifying Domain Name Ownership	Yes, see above
Verifying Email Address Control	Yes, see above
Verifying Identity of Code Signing Certificate Subscriber	Yes, see above
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	?

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

Long-lived DV certificates	SSL certs are OV or EV. 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	Wildcard certs are allowed for OV certs, not for EV certs.
Email Address Prefixes for DV Certs	SSL certs are OV.
Delegation of Domain / Email validation to third parties	?
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	?
Distributing generated private keys in PKCS#12 files	?
Certificates referencing hostnames or private IP addresses	?
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	?
CRL with critical CIDP Extension	?
Generic names for CAs	No
Lack of Communication With End Users	No