Mozilla - CA Program

Case Information

Case Number	00000047	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	TurkTrust	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	TurkTrust Root Renewal Request	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1007683

General information about CA's associated organization

Company Website	http://www.turktrust.com.tr/en	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Turkey	**Verified?**	Verified
Primary Market / Customer Base	TURKTRUST issues certificates to the public.	**Verified?**	Verified
Impact to Mozilla Users	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. One of TURKTRUST's previously included root certs expires this November	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* Revocation of Compromised Certificates: Yes. CPS section 4.9.1 *DNS names go in SAN: Yes. CPS section 3.1.5.1: "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	**Verified?**	Verified

field. The constraints which are specified in “CN” are also valid for SAN field.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	https://bugzilla.mozilla.org/show_bug.cgi?id=1007683#c8 * CPS section 6.3.2: The term for 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 electronic certificates 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. *CPS section 3.1.5.1: 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. Wildcards are not issued for EV SSL certificates. * The following e-mail address prefixes are used for domain verification of both DV and OV certificates: "admin", "administrator", "webmaster", "hostmaster" or "postmaster". * Domain/e-mail validation is performed by TURKTRUST CA and is not delegated to any third party. * We are not issuing any new SHA-1 intermediate or end-entity certificates and we do not have any active SHA-1 intermediate certificates in use.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5	**Root Case No**	R00000062
Request Status	Ready for Public Discussion	**Case Number**	00000047

Additional Root Case Information

Subject	Include TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5 root

Technical Information about Root Certificate

O From Issuer Field	TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	The H5 root has internally-operated subCAs that issue SSL and Code Signing certificates.	**Verified?**	Verified
Root Certificate Download URL	http://www.turktrust.com.tr/sertifikalar /TURKTRUST_Elektronik_Sertifika_Hizmet_Saglayicisi_h5.crt	**Verified?**	Verified
Valid From	2013 Apr 30	**Verified?**	Verified
Valid To	2023 Apr 28	**Verified?**	Verified

Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://testsuite12001.turktrust.com.tr	**Verified?**	Verified
CRL URL(s)	http://www.turktrust.com.tr/sil/TURKTRUST_SSL_SIL_h5.crl http://www.turktrust.com.tr/sil/TURKTRUST_Kok_SIL_h5.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.turktrust.com.tr	**Verified?**	Verified
Trust Bits	Code; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	C4:18:F6:4D:46:D1:DF:00:3D:27:30:13:72:43:A9:12:11:C6:75:FB	**Verified?**	Verified
SHA-256 Fingerprint	49:35:1B:90:34:44:C1:85:CC:DC:5C:69:3D:24:D8:55:5C:B2:08:D6:A8:14:13:07:69:9F:4A:F0:63:19:9D:78	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	http://www.turktrust.com.tr/en/bilgi-deposu/kok-sertifikalari-kurulumu-ve-iptal-listeleri/ 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	**Verified?**	Verified
Externally Operated SubCAs	None. None planned.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third-party issuers.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Turkish & English English versions:	**Verified?**	Verified

	CP (QEC): http://dl.turktrust.com.tr/pdf/TURKTRUST-CP-v09-QEC.pdf CPS (QEC): http://dl.turktrust.com.tr/pdf/TURKTRUST-CPS-v09-QEC.pdf CP (SSL, EVSSL, NIMS etc.): http://dl.turktrust.com.tr/pdf/TURKTRUST-CP-v09-SSL.pdf CPS (SSL, EVSSL, NIMS etc.): http://dl.turktrust.com.tr/pdf/TURKTRUST-CPS-v09-SSL.pdf		
CA Document Repository	http://www.turktrust.com.tr/en/bilgi-deposu	**Verified?**	Verified
CP Doc Language	English		
CP	http://dl.turktrust.com.tr/pdf/TURKTRUST-CP-v09-SSL.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://dl.turktrust.com.tr/pdf/TURKTRUST-CP-v09-SSL.pdf	**Verified?**	Verified
Other Relevant Documents	SSL Certificate Services Declaration: http://dl.turktrust.com.tr/pdf/DOCUMENT-SSL-LetterOfCommitment.pdf SSL Certificate Owner Declaration: http://dl.turktrust.com.tr/pdf/DOCUMENT-SSL-Subscriber.pdf Law and Regulations (Turkish): http://www.turktrust.com.tr/tr/bilgi-deposu/kanun-teblig-ve-yonetmelikler/	**Verified?**	Verified
Auditor Name	TUVIT	**Verified?**	Verified
Auditor Website	https://www.tuvit.de	**Verified?**	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	**Verified?**	Verified
Standard Audit	https://www.tuvit.de/en/certification-overview-1265-trusted-site-etsi-certificates-1334.htm	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	12/19/2014	**Verified?**	Verified
BR Audit	https://www.tuvit.de/en/certification-overview-1265-trusted-site-etsi-certificates-1334.htm	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	12/19/2014	**Verified?**	Verified
EV Audit	https://www.tuvit.de/en/certification-overview-1265-trusted-site-etsi-certificates-1334.htm	**Verified?**	Verified
EV Audit Type	ETSI TS 102 042	**Verified?**	Verified
EV Audit Statement Date	12/19/2014	**Verified?**	Verified
BR Commitment to Comply	CPS and CP section 1	**Verified?**	Verified
SSL Verification Procedures	Domain/e-mail validation is performed by TURKTRUST CA and is not delegated to any third party. The following e-mail address prefixes are used for domain verification: "admin", "administrator", "webmaster", "hostmaster" or "postmaster". CPS section 3.2.2.1. 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, different control steps are applied depending on whether the request is domestic or	**Verified?**	Verified

	foreign. The residential address of the subscriber is based on while determining of such distinction. Subscribers' legal existence and credentials, domain name, applicant's representative's and application's existence, CSR information and so forth informations 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 SSL Verification Procedures	Not requesting EV treatment for this root.	**Verified?**	Not Applicable
Organization 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. CPS section 3.2.4. Validation of Authority: For SSL and EV SSL applications and in such case if the subscriber is a legal entity for an OSC application, the existence of the applicant's representative and the existence of the application are verified via an independent information source as specified in TURKTRUST procedures.	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the Email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	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. 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. Section 3.1.5.3. 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. Section 3.2.2: In cases where a certificate contains the name of a legal entity shall be verified against the official documents of the country of residence of the applicant. 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. For SSL and OSC applications, different control steps are applied depending on whether the request is domestic or foreign. The residential address of the subscriber is based on while determining of such distinction. Subscribers' legal	**Verified?**	Verified

	existence and credentials, domain name, applicant's representative's and application's existence, CSR information and so forth informations should be verified This verification is done with a unique user name and activation code sent to the authorized person's e-mail address.		
Multi-Factor Authentication	We confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance.	**Verified?**	Verified
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	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.turktrust.com.tr/en/bilgi-deposu/kok-sertifikalari-kurulumu-ve-iptal-listeleri/	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H6	**Root Case No**	R00000063
Request Status	Ready for Public Discussion	**Case Number**	00000047

Additional Root Case Information

Subject	Include TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H6 root

Technical Information about Root Certificate

O From Issuer Field	TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	The H6 root has an internally-operated subCA that issues EV SSL certificates.	**Verified?**	Verified
Root Certificate Download URL	http://www.turktrust.com.tr/sertifikalar/TURKTRUST_Elektronik_Sertifika_Hizmet_Saglayicisi_h6.crt	**Verified?**	Verified
Valid From	2013 Dec 18	**Verified?**	Verified
Valid To	2023 Dec 18	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL)	https://testsuite12002.turktrust.com.tr	**Verified?**	Verified

or Example Cert			
CRL URL(s)	http://www.turktrust.com.tr/sil/TURKTRUST_EV_SSL_SIL_h6.crl http://www.turktrust.com.tr/sil/TURKTRUST_Kok_SIL_h6.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.turktrust.com.tr	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
EV Policy OID(s)	2.16.792.3.0.3.1.1.5	**Verified?**	Verified
EV Tested	// CN=TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H6,O=TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A...,L=Ankara,C=TR "2.16.792.3.0.3.1.1.5", "TurkTrust EV OID", SEC_OID_UNKNOWN, { 0x8D, 0xE7, 0x86, 0x55, 0xE1, 0xBE, 0x7F, 0x78, 0x47, 0x80, 0x0B, 0x93, 0xF6, 0x94, 0xD2, 0x1D, 0x36, 0x8C, 0xC0, 0x6E, 0x03, 0x3E, 0x7F, 0xAB, 0x04, 0xBB, 0x5E, 0xB9, 0x9D, 0xA6, 0xB7, 0x00 }, "MIGxMQswCQYDVQQGEwJUUjEPMA0GA1UEBwwGQW5rYXJhMU0wSwYDVQQKDERUw5xS" "S1RSVVNUIEJpbGdpIMSwbGV0acWfaW0gdmUgQmlsacWfaW0gR8O8dmVubGnEn2kg" "SGl6bWV0bGVyaSBBLsWeLjFCMEAGA1UEAww5VMOcUktUUlVTVCBFbGVrdHJvbmlr" "IFNlcnRpZmlrYSBIaXptZXQgU2HEn2xhecSxY8Sxc8SxIEg2", "faHyZeyK", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	8A:5C:8C:EE:A5:03:E6:05:56:BA:D8:1B:D4:F6:C9:B0:ED:E5:2F:E0	**Verified?**	Verified
SHA-256 Fingerprint	8D:E7:86:55:E1:BE:7F:78:47:80:0B:93:F6:94:D2:1D:36:8C:C0:6E:03:3E:7F:AB:04:BB:5E:B9:9D:A6:B7:00	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	http://www.turktrust.com.tr/en/bilgi-deposu/kok-sertifikalari-kurulumu-ve-iptal-listeleri/ TURKTRUST ECSP 6. ROOT HIERARCHY Root: TURKTRUST Electronic Certificate Service Provider Certificate EV SSL subCA: TURKTRUST Electronic Server Certificate Services Certificate (EVSSL)	**Verified?**	Verified
Externally Operated SubCAs	None. None planned.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third-party issuers.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Turkish & English	**Verified?**	Verified
CA Document Repository	http://www.turktrust.com.tr/en/bilgi-deposu	**Verified?**	Verified
CP Doc Language	English		
CP	http://dl.turktrust.com.tr/pdf/TURKTRUST-CP-v09-SSL.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://dl.turktrust.com.tr/pdf/TURKTRUST-CP-v09-SSL.pdf	**Verified?**	Verified
Other Relevant Documents	SSL Certificate Services Declaration: http://dl.turktrust.com.tr/pdf/DOCUMENT-SSL-LetterOfCommitment.pdf SSL Certificate Owner Declaration: http://dl.turktrust.com.tr/pdf/DOCUMENT-SSL-Subscriber.pdf Law and Regulations (Turkish): http://www.turktrust.com.tr/tr/bilgi-deposu/kanun-teblig-ve-yonetmelikler/	**Verified?**	Verified
Auditor Name	TUVIT	**Verified?**	Verified
Auditor Website	https://www.tuvit.de	**Verified?**	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	**Verified?**	Verified
Standard Audit	https://www.tuvit.de/en/certification-overview-1265-trusted-site-etsi-certificates-1334.htm	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	12/19/2014	**Verified?**	Verified
BR Audit	https://www.tuvit.de/en/certification-overview-1265-trusted-site-etsi-certificates-1334.htm	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	12/19/2014	**Verified?**	Verified
EV Audit	https://www.tuvit.de/en/certification-overview-1265-trusted-site-etsi-certificates-1334.htm	**Verified?**	Verified
EV Audit Type	ETSI TS 102 042	**Verified?**	Verified
EV Audit Statement Date	12/19/2014	**Verified?**	Verified
BR Commitment to Comply	CPS and CP section 1	**Verified?**	Verified
SSL Verification Procedures	Domain/e-mail validation is performed by TURKTRUST CA and is not delegated to any third party. The following e-mail address prefixes are used for domain verification: "admin", "administrator", "webmaster", "hostmaster" or "postmaster". CPS section 3.2.2.1. 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, different control steps are applied depending on whether the request is domestic or foreign. The residential address of the subscriber is based on while determining of such distinction. Subscribers' legal existence and credentials, domain name, applicant's	**Verified?**	Verified

	representative's and application's existence, CSR information and so forth informations 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 SSL Verification Procedures	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.	**Verified?**	Verified
Organization 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. CPS section 3.2.4. Validation of Authority: For SSL and EV SSL applications and in such case if the subscriber is a legal entity for an OSC application, the existence of the applicant's representative and the existence of the application are verified via an independent information source as specified in TURKTRUST procedures.	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the Email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit for this root.	**Verified?**	Not Applicable

Multi-Factor Authentication	We confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance.	**Verified?**	Verified
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	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.turktrust.com.tr/en/bilgi-deposu/kok-sertifikalari-kurulumu-ve-iptal-listeleri/	**Verified?**	Verified