Print this page

Mozilla - CA Program

Case Information

Case Number	00000078	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Turkey, Kamu Sertifikasyon Merkezi (Kamu SM)	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include renewed Kamu SM root certificate	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1262809

General information about CA's associated organization

CA Email Alias 1	eit@kamusm.gov.tr		
CA Email Alias 2	cainfo@kamusm.gov.tr		
Company Website	http://www.kamusm.gov.tr/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Turkey	**Verified?**	Verified
Primary Market / Customer Base	Public Certification Authority of Turkey	**Verified?**	Verified
Impact to Mozilla Users	Kamu SM (Government Certification Authority) is a government-owned Certificate Authority (CA) in Turkey operated in compliance with the international standards.	**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	* Publicly Available CP and CPS: Yes. http://depo.kamusm.gov.tr/ilke/ * CA Hierarchy: Yes. CP/CPS Section 1.3.1: This root certificate has one internally operated subordinate CA that issues end-entity certificates for only SSL. * Audit Criteria: Yes. audit report from ICTA. ICTA is declared as the regularity and auditing body for electronic certificate service providers in Turkey by the Turkish Electronic Signature Law. And also according to section 10 and 11 of Mozilla's CA Certificate Inclusion Policy, our audit report states that our government CA complies with ETSI TS 101 456, ETSI TS 102 042 and CA/Browser Forum Baseline Requirements. * Document Handling of IDNs in CP/CPS: CA does not allow the use of internationalized domain names (IDNs) * Revocation of Compromised Certificates: CP/CPS Section 4.9.1 explains all the conditions of revocation. * Verifying Domain Name Ownership: CP/CPS Section 3.2.2 explains the procedure in details. * Verifying Email Address Control: CP/CPS Section 3.2.2 explains the procedure in details. * DNS names go in SAN: CP/CPS Section 3.1.5 * Domain owned by a Natural Person: CA does not issue certificates to natural persons. * OCSP: CP/CPS Section 4.1.9	**Verified?**	Verified

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	* Long-lived DV certificates: CP/CPS Section 6.3.2: The public and private keys of the server certificate may be valid for up to three years from the date they were validated. * Wildcard DV SSL certificates: CA does not issue DV certificates. * Email Address Prefixes for DV Certs: CA does not issue DV certificates. * Delegation of Domain / Email validation to third parties: No. CA does not employ third parties in any way. * Issuing end entity certificates directly from roots: No. End entity SSL certificates are issued from Subordinate CA. * Allowing external entities to operate subordinate CAs:	**Verified?**	Verified

No.Subordinate CAs are internally operated.
* Distributing generated private keys in PKCS#12 files: No. CA does not generate key pair, it is generated by the applicant as written in CP/CPS Section 6.1.1.
* Certificates referencing hostnames or private IP addresses: No. CA does not issue certificates referencing hostnames or private IP addresses as written in CP/CPS Section 3.1.5
* Issuing SSL Certificates for Internal Domains: No. CA does not issue certificates for internal domains as written in CP/CPS Section 3.1.5
* OCSP Responses signed by a certificate under a different root: No. OCSP responses are signed under the same root.
* Generic names for CAs : No. Root CA is named as “TUBITAK Kamu SM SSL Kok Sertifikası – Surum 1” and has one subordinate CA with the name “TUBITAK Kamu SM SSL Sertifika Hizmet Sağlayıcısı-Sürüm 1”.
* Lack of Communication With End Users: CA is contactable by, and accept and act upon complaints made by, those relying on their assertions of identity. CA has a call center for communication. (Call center number: +90 262 648 18 00)

Root Case Record # 1

Root Case Information

Root Certificate Name	TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	**Root Case No**	R00000113
Request Status	Ready for Public Discussion	**Case Number**	00000078

Certificate Data

Certificate Issuer Common Name	TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1
O From Issuer Field	Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK
OU From Issuer Field	Kamu Sertifikasyon Merkezi - Kamu SM
Valid From	2013 Nov 25
Valid To	2043 Oct 25
Certificate Serial Number	01
Subject	CN=TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1, OU=Kamu Sertifikasyon Merkezi - Kamu SM, O=Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK, C=TR
Signature Hash Algorithm	sha256WithRSAEncryption

Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	31:43:64:9B:EC:CE:27:EC:ED:3A:3F:0B:8F:0D:E4:E8:91:DD:EE:CA
SHA-256 Fingerprint	46:ED:C3:68:90:46:D5:3A:45:3F:B3:10:4A:B8:0D:CA:EC:65:8B:26:60:EA:16:29:DD:7E:86:79:90:64:87:16
Certificate Fingerprint	FC:7E:0F:2A:69:65:CF:D6:EE:CB:49:65:EB:14:C6:F9:98:6B:FC:46:6C:FD:E9:A4:84:3B:7C:BD:83:BF:77:0E
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This is the SHA-2 version of the "TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3" root cert that was included via Bugzilla Bug #381974. It has one internally-operated subCA that issues OV SLL certificates to major government entities in Turkey.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8738995 http://depo.kamusm.gov.tr /ssl/SSLKOKSM.S1.cer	**Verified?**	Verified
CRL URL(s)	http://depo.kamusm.gov.tr /ssl/SSLSIL.S1.crl http://depo.kamusm.gov.tr /ssl/SSLKOKSIL.S1.crl SSL CP/CPS Section 4.9.7: CRL for end-entity certs is valid for maximum of 36 hours.	**Verified?**	Verified
OCSP URL(s)	http://ocspssls1.kamusm.gov.tr http://ocspsslkoks1.kamusm.gov.tr	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	*.gov.tr, *.k12.tr, *.pol.tr, *.mil.tr, *.tsk.tr, *.kep.tr,*.bel.tr,*.edu.tr, *.org.tr	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://testssl.kamusm.gov.tr/	**Verified?**	Verified

Test Website - Expired	
Test Website - Revoked	

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/testssl.kamusm.gov.tr lists error: NextUpdate not set (RFC 5019, section 2.2.4). According to rfc6960 the nextUpdate value is optional, but according to rfc5019 (OCSP Profile for High-Volume Environments) it's required. The revocationcheck site is tuned CA's for high volume environments. ComSign chooses to abide by rfc6960 in which NextUpdate is optional	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/ returning "Certificate not found."	**Verified?**	Verified
Test Website Lint Test	https://cert-checker.allizom.org/ No errors. Warning: Serial numbers should have at least 20 bits of entropy	**Verified?**	Verified
EV Tested	Not requesting EV treatment.	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	SSL CP/CPS Section 1.3.1: This root certificate has internally operated subordinate CAs that issue SSL end-entity certificates.	**Verified?**	Verified
Externally Operated SubCAs	None. None planned.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No such third party exists. SSL CP/CPS section 1.3.2: All registration procedures are directly executed by Kamu SM personnel.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Turkish. The SSL CP/CPS has been translated into English. Certificates: http://www.kamusm.gov.tr/depo/sertifikalar/depo.jsp	**Verified?**	Verified

	CP (Turkish): http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SI/KSM_NES_SI.pdf CPS (Turkish): http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SUE/KSM_NES_SUE.pdf		
CA Document Repository	http://depo.kamusm.gov.tr/ilke/	**Verified?**	Verified
CP Doc Language	Turkish		
CP	http://depo.kamusm.gov.tr/ilke/KamuSM_CPS/KamuSM_CPS_Tr.pdf	**Verified?**	Verified
CP Doc Language	Turkish		
CPS	http://depo.kamusm.gov.tr/ilke/KamuSM_CPS/KamuSM_CPS_En.pdf	**Verified?**	Verified
Other Relevant Documents	Audit certificate: http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fSectors%2f%C4%B0nformation+Technologies+Sector%2fTUB%C4%B0TAK+yetkilendirme.pdf	**Verified?**	Verified
Auditor Name	Information and Communications Technologies Authority (ICTA)	**Verified?**	Verified
Auditor Website	http://www.btk.gov.tr/tr-TR/Anasayfa	**Verified?**	Verified
Auditor Qualifications	http://www.btk.gov.tr/en-US/	**Verified?**	Verified
Standard Audit	https://bug1262809.bmoattachments.org/attachment.cgi?id=8819839	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	12/19/2016	**Verified?**	Verified
BR Audit	https://bug1262809.bmoattachments.org/attachment.cgi?id=8819839	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	12/19/2016	**Verified?**	Verified
EV Audit	Not requesting EV treatment	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1	**Verified?**	Verified
SSL Verification Procedures	SSL CP/CPS section 3.2.2: Verification procedures of Kamu SM shall be performed in compliance with the following steps: ... It should be verified that e-mail address declared by organization representative having applied for certificate	**Verified?**	Verified

	during application is sent by the organization representative. This verification procedure shall be confirmed by a verification e-mail sent to e-mail address of organization representative. • WHOIS records pertinent to domain name specified in certificate application shall be verified via "www.nic.tr " • As a principle, applicant should have exclusive right and authority in regard to use of relevant domain name which is included in the certificate. This exclusive right and authority must be granted by registered owner or organization of domain name. ...		
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	SSL CP/CPS document Section 3.2.2, Authentication of Organization Identity	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the Email trust bit	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	After the verification of certificate issuance, the Kamu SM Operator login to the Kamu SM Certificate Issuance system by using authorized smart card and password. Then operates the Kamu SM system. So, We confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. SSL CP/CPS section 5.2.	**Verified?**	Verified
Network Security	Kamu SM network security processes and infrastructure meets "CA / Browser Forum Network and Certificate System Security Requirements, v. 1". Our security operation center (SOC) has capability to monitor all infrastructure and capture full packet data of last 2 week. Therefore our information security analyst have ability to perform detailed network forensics. Software and signature of all security systems such as IPS, IDS, SIEM etc. are updated periodically. SSL CP/CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.kamusm.gov.tr/depo/sertifikalar/depo.jsp	**Verified?**	Verified