Bugzilla ID: 381974
Bugzilla Summary: Add Kamu Sertifikasyon Merkezi CA root certificate

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.

General Information	**Data**
CA Name	Kamu SM Kamu Sertifikasyon Merkezi
Website URL	http://www.kamusm.gov.tr/en/
Organizational type.	Government Organization that works with private and public corporations.
Primary market / customer base.	Kamu Sertifikasyon Merkezi is a national government CA in Turkey that has authorization to issue certificates to government entities and commercial companies. Kamu SM is part of The National Research Institute of Electronics and Cryptology (Turkish: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - **UEKAE**), which is a subsidiary of The Scientific and Technological Research Council of Turkey (Turkish: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK) UEKAE is a national scientific organization with the aim of developing advanced technologies for information security. UEKAE produces projects in partnership with public and private sector organizations and ensures participation of universities in these projects. In addition, the institute responds to the national needs in the fields of information security and advanced electronics technologies.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3
Cert summary / comments	This root has two internally-operated subordinated CAs. One is for issuing certificates for secure signature. The other is for issuing certificates for logging on domains, databases, applications and www; protection of e-mails; protection of SSL servers; development of the VPNs; protection and signing of software.
Root CA certificate URL	http://www.kamusm.gov.tr/BilgiDeposu/KOKSHS.v3.crt
SHA-1 fingerprint.	1B:4B:39:61:26:27:6B:64:91:A2:68:6D:D7:02:43:21:2D:1F:1D:96
Valid from	8/24/2007
Valid to	8/21/2017
Cert Version	3
Modulus length	2048

CRL URL update frequency for end-entity certificates	http://www.kamusm.gov.tr/BilgiDeposu/KOKSIL.v3.crl “We issue the CRLs with 24hr periods and after every hold and revocation process” http://www.kamusm.gov.tr/BilgiDeposu/CSHSIL.v3.crl NextUpdate: 24 hours
OCSP Responder URL	http://ocsp.kamusm.gov.tr/
List or description of subordinate CAs operated by the CA organization associated with the root CA.	Cert hierarchy diagram: http://www.kamusm.gov.tr/en/hiyerarsi.jpg There are 2 subordinate CAs (section 1.1 of CP) 1) Cihaz Sertifikasi Hizmet Sağlayıcısı - Sürüm 3 Device Certificate Service Provider http://www.kamusm.gov.tr/BilgiDeposu/CSHS.v3.crt Issues qualified electronic certificates for logging on domains, databases, applications and www; protection of e-mails; protection of SSL servers; development of the VPN's; protection and signing of software) 2) Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 Public Electronic Certificate Service Provider http://www.kamusm.gov.tr/BilgiDeposu/NESHS.v3.crt Issues Qualified electronic certificates for secure-signature
Externally operated sub CAs	No subordinate CAs operated by third parties.
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Email
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV
EV policy OID	Not EV
For SSL certificates: URLs of one or more web servers using the certificate(s).	https://mail.rtuk.org.tr

CP/CPS	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 English Translations of parts of CPS https://bugzilla.mozilla.org/attachment.cgi?id=331075
AUDIT	Audit Type: ETSI TS 101.456 Auditor: Turkish Telecommunications Authority Auditor Website: http://www.tk.gov.tr/, http://www.tk.gov.tr/eimza/eshs.htm Statement of ETSI Compliance: http://www.tk.gov.tr/eimza/doc/aciklama/tubitak.jpg (2007.06.18) Letter from auditor: https://bugzilla.mozilla.org/attachment.cgi?id=372010 Comment #51: The Frequency of our ETSI audit is one of every two years or when if major changes come up. Additionally, we have had a date to new audit. It will be in first quarter of this May. After that we will send the report, immediately.

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - "CP/CPS Section 3.2.2-Determination of Corporate Identity: Determination of Corporate Identity of the public institutions' that request SSL certificates from Kamu SM is done by official correspondence between institutions and domain name that is given in the certificate request is verified through the proper channels(nic.tr)."
    - "CP/CPS Sections 3.2.3 / 3.2.5-Determination of Personal Identity / Verification of Authority: The person that requests a SSL certificate from Kamu SM must have authority to request a certificate for the domain name that is used in the certificate request. This authority is verified by official correspondence with the public institution."
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - "CP/CPS Sections 3.2.3 / 3.2.5-Determination of Personal Identity / Verification of Authority: To verify the email account associated with the email address in the certificate, email is sent to reach the person for verification. In the email field, email addresses that has the institution's domain name are accepted only. To verify the subscriber's legal identity their national identification number is taken in the application form which is approved by the director of the institution."

- Verify identity info in code signing certs is that of subscriber
    - “Currently we do not give code signing certificates.”
- Other
    - “Section 3 of the CP/CPS is for Identification and Authentication. The checks are done by our certificate creation software, which is programmed to work according to policies given in RFC 3647.
    - Section 3.1.1 Domain Name Types- In the certificates given by Kamu SM, the DN(Distinguished Name) field which holds the subscribers identity information must comply with the “ITU X.500” name types.
    - Section 3.1.2 Identity information to be recognizable- Identity information that is on the certificate must be meaningful to determine the real or legal entity(name, surname, company name, email address).
    - Section 3.1.3 Use of nicknames for the subscriber- In the certificate content no nicknames are allowed for the subscriber.
    - Section 3.1.4 Interpretation of different name forms- In the certificate content name forms other than “ITU X.500” cannot be used.
    - Section 3.1.5 Uniqueness of identity information- Every certificate given by Kamu SM has distinguishing attributes for the real or legal entities. Same real or legal entity may use the same identity information in certificates but for different entities using same information is not allowed.
    - Section 3.1.6 Recognition, authentication, and role of trademarks- Applicants who apply for a certificate from Kamu SM may not use names that would harm others' intellectual and industrial property rights. Kamu SM does not verify whether the names used in the certificates are damage to others' intellectual and industrial property rights. If there is a problem with the intellectual and industrial property rights, Kamu SM holds the right to decline the certificate application or to revoke the certificates it has given. Kamu SM does not take mediation actions to solve the intellectual and industrial property rights problems.”

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - SSL certs are OV.
    - “We give SSL certificates for 1 year and 3 years.”
- Wildcard DV SSL certificates
    - SSL certs are OV.
    - “Wildcard certificates have been given only to public institutions.”
- Delegation of Domain / Email validation to third parties
    - “We generate certificates only in our center.”
- Issuing end entity certificates directly from roots
    - End-entity certs are issued through intermediate CAs, and not directly by the root.

- Allowing external entities to operate unconstrained subordinate CAs
    - No subordinate CAs operated by third parties.
- Distributing generated private keys in PKCS#12 files
    - "We don't use this method. We prefer our customers create their own keys and we use 2 different secure channel to deliver the certificate to them. Their private key never come to us."
- Certificates referencing hostnames or private IP addresses
    - "We don't create such this certificates. We create for only authorized domain names that customer has to prove it with official papers."
- OCSP Responses signed by a certificate under a different root
    - "We don't use OCSP for SSL certificates. If we do in future, we would just use our own OCSP services and not provide to respond for other root certificates."
- CRL with critical CIDP Extension
    - CRLs downloaded into Firefox without error.
- Generic names for CAs
    - "We don't let usage of generic names in CA certificates. All of them have unique names."

Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
    - On Turkish Telecommunications Authority website
- For EV CA's, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issues noted in the report