**Bugzilla ID:** To be assigned

**Bugzilla Summary:** To be filled

**General information  about  the  CA’s  associated  organization**

|  |  |
| --- | --- |
| CA  Company  Name   |  Kamu Sertifikasyon Merkezi (Kamu SM)  |
| Website  URL   | <http://www.kamusm.gov.tr/> (Turkish Only) |
| Organizational  type   | National Government |
| Primark  Market  /  Customer  Base   | Kamu Sertifikasyon Merkezi (Kamu SM) is the Government Certification Authority formed by Informatics and Information Security Research Center (BİLGEM) of The Scientific and Technological Research Council of Turkey (TÜBİTAK). CA will issue SSL certificates to a large number of government entities in Turkey. There is no government CA in Turkey other than Kamu SM. But there are any other private agencies serving SSL certificates to public. Our CA will issue certificates only in our country, Turkey.  |
| Impact  to  Mozilla  Users   | The Turkish Government decided to centralize government certification system and therefore Kamu SM is the only government certification authority in Turkey. Besides Kamu SM has a root in major browsers and aim is to renew existing root because of SHA-1 sunset. Mozilla users are likely to encounter root certificate as relying parties while web browsing (HTTPs servers doing SSL). |
| Inclusion  in  other  major  browsers   | Currently CA has a root included to the stores of Mozilla and Microsoft which is named “TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3” and has a SHA-1 thumbprint as 1b 4b 39 61 26 27 6b 64 91 a2 68 6d d7 02 43 21 2d 1f 1d 96 . Now, we are working to add our renewed root to Mozilla, Microsoft and Apple (Safari). This new root certificate has been created in order to comply with Baseline Requirements and renewed because of SHA-1 sunset. New root will eventually replace “TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3” root certificate. |
| CA  Primary  Point  of  Contact  (POC)   | * A direct E-mail address: tugba.ozcan@kamusm.gov.tr
* CA Email Alias: eit@kamusm.gov.tr, emrah.durmaz@kamusm.gov.tr, senol.senyurt@kamusm.gov.tr , yusuf.usta@kamusm.gov.tr
* CA Phone Number: +90 262 648 18 00 / 8543 or +90 5069862600
* Title / Department: E-Signature Infrastructure Department
 |

**Technical information  about  each  root**certificate

|  |  |
| --- | --- |
| Certificate  Name   | TUBITAK Kamu SM SSL Kok Sertifikası – Surum 1 |
| Certificate  Issuer  Field   | CN = TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1OU = Kamu Sertifikasyon Merkezi - Kamu SMO = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAKL = Gebze - KocaeliC = TR |
| Certificate  Summary   | This is the SHA-2 version of currently included root “TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3”. We only update the signature algorithm RSA with SHA1 to RSA with SHA-256.Our purpose is issuing OV SLL certificates to major government entities in Turkey. |
| Mozilla Applied Constraints | \*.gov.tr, \*.k12.tr, \*.pol.tr, \*.mil.tr, \*.tsk.tr, \*.kep.tr,\*.bel.tr,\*.edu.tr, \*.org.tr |
| Root  Cert  URL   | http://depo.kamusm.gov.tr/ssl/SSLKOKSM.S1.cer   |
| SHA1  Fingerprint   | ‎ ‎31 43 64 9b ec ce 27 ec ed 3a 3f 0b 8f 0d e4 e8 91 dd ee ca |
| Valid  From     | 25.11.2013 |
| Valid  To     | 25.10.2043 |
| Certificate  Version   |  v3 |
| Certificate  Signature  Algorithm   | RSA with SHA-256   |
| Signing  key  parameters   |  |
| Test  Website  URL  (SSL)  Example  Certificate  (non-­‐SSL)   | testssl.kamusm.gov.tr |
| CRL  URL   | <http://depo.kamusm.gov.tr/ssl/SSLSIL.S1.crl>CP/CPS Section 4.9.7: Each CRL issued by Kamu SM contains entries for all revoked Certificates and is valid for 36 hours. Kamu SM issues a new CRL every 12 hours and each CRL issued has a monotonically increasing sequence number. |
| OCSP URL | <http://ocspssls1.kamusm.gov.tr>OCSP responder is sourced by database which is updated instantly. So CA reflects the revocation of an end entity or CA certificate momently. Testing Result: Browsing to test website with OCSP enforced in Firefox browser. |
| Requested  Trust Bits   |  Websites (SSL/TLS)     |
| SSL  Validation  Type   | OV |
| EV  Policy  OID(s)   | N/A   |
| Non-­‐sequential  serial  numbers  and  entropy  in  cert   | Available |

**CA Hierarchy  information  for  each  root  certificate**

|  |  |
| --- | --- |
| CA  Hierarchy   | CP/CPS Section 1.3.1: This root certificate has one internally operated subordinate CA that issues end-entity certificates for only SSL.  |
| Externally  Operated  SubCAs   | N/A |
| Cross-­‐Signing   | N/A   |
| Technical  Constraints  on  Third-­‐party  Issuers   | No such third party exists   |

|  |  |
| --- | --- |
| Policy  Documentation   | Language(s)  that  the  documents are in: CP: (Turkish & English)CPS: (Turkish & English)Relying Agreements: (Turkish only) |
| Audits   | Auditor: Information and Communications Technologies Authority (ICTA) Audit Type: According to sections 9 of Mozilla’s CA Certificate Inclusion Policy, our CA had an 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.The last audit date was April, 30.12.2015 Auditor  Website:  <http://www.btk.gov.tr/tr-TR/Anasayfa> Certificate URL: <http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fSectors%2f%C4%B0nformation+Technologies+Sector%2fTUB%C4%B0TAK+yetkilendirme.pdf> |
| Baseline  Requirements  (SSL)   | Audit report states that our government CA complies with CA/Browser Forum Baseline Requirements. |
| SSL  Verification  Procedures   |  CPS Section 3.2.2, CPS Section 3.25 and CPS Section 4.2.1 explains all the SSL verification procedure briefly. As a summary:  To guarantee that an applicant government entity has control over the domain (URL) which will be subject field of requested certificate, these types of checks are performed: - Organizational checks: the ownership title of the domain name is requested and is certified by a legal representative of the organization. - Technical checks: For \*.gov.tr, \*.k12.tr, \*.pol.tr, \*.mil.tr, \*.tsk.tr, \*.kep.tr,\*.bel.tr,\*.edu.tr, \*.org.tr domains, WHOIS services are used to search via https://www.nic.tr.  |
| Organization  Verification  Procedures   |  CP/CPS document Section 3.2.2, Authentication of Organization Identity explains briefly. |
| Email  Address  Verification  Procedures   | CA does not enable the Email (S/MIME) trust bit.    |
| Code  Signing  Subscriber  Verification  Procedures   | CA does not perform code signing |
| 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  certificateIssuance |
| 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. In additional to these, following requirements are completed;• Maintain network security controls that at minimum meet the CA/B Forum Network and Certificate System Security Requirements. • Check for mis-issuance of certificates, especially for high-profile domains. • Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. • Ensure Intrusion Detection System and other monitoring software is up-to-date. • Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion. |

**Verification  Policies  and  Practices**

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

|  |  |
| --- | --- |
| Publicly  Available  CP  and  CPS   |  OK. http://depo.kamusm.gov.tr/ilke/ |
| CA  Hierarchy   |  OK. 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   |  OK.  According to sections 9 of Mozilla’s CA Certificate Inclusion Policy, our CA had an 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   | No. CA does not allow the use of internationalized domain names (IDNs) |
| Revocation  of  Compromised  Certificates   |  OK. CP/CPS Section 4.9.1 explains all the conditions of revocation.   |
| Verifying  Domain  Name  Ownership   | OK. CP/CPS Section 3.2.2 explains the procedure in details. |
| Verifying  Email  Address  Control   |   OK. CP/CPS Section 3.2.2 explains the procedure in details. |
| Verifying  Identity  of  Code  Signing  Certificate  Subscriber   |  NO. CA does not issue Code Signing Certificate. |
| DNS  names  go  in  SAN   |  OK. CP/CPS Section 3.1.5 explains the procedure in details. |
| Domain  owned  by  a  Natural  Person   |  NO.CA does not issue certificates to natural persons. |
| OCSP   |   OK. CP/CPS Section 4.1.9 explains the procedure in details. |

**Response to Mozilla's list of Potentially Problematic Practices (**[**https://wiki.mozilla.org/CA:Problematic\_Practices**](https://wiki.mozilla.org/CA%3AProblematic_Practices) **)**

|  |  |
| --- | --- |
| Long-lived DV certificates  | OK. CP/CPS Section 6.3.2: The public and private keys of the server certificate shall be valid for three years from the date they were validated. |
| Wildcard DV SSL certificates |  No. CA does not issue DV certificates. |
| Email Address Prefixes for DV Certs |  No. 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 |  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 6.1.1.2 |
| 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 | OK. 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 ) |