PUBLIC

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM PKI DISCLOSURE STATEMENT

Document Code
PRO.01.02

Version No
00

Issue/Revision Date
22.10.2018

PUBLIC

KAMU SM PKI DISCLOSURE STATEMENT

DOCUMENT PREPARATION HISTORY		
Version No	**Reason for Release**	**Issue Date**
00	Initial Release	22.10.2018

CONTENTS

1 Introduction

Kamu SM (Government Certification Authority) was founded in accordance with Electronic Signature Law no. 5070 dated January 15th, 2004 by The Scientific and Technological Research Council of Turkey (TÜBİTAK). Kamu SM is a government-owned Certificate Authority (CA) operated in compliance with the international standards.

Referred as PKI Disclosure Statement (PDS), this document has been prepared following the structure of ETSI EN 319 411-1 (Annex A).

It is a supplemental instrument of disclosure and notice by Kamu SM to Subscribers and Relying Parties and does not replace or substitute the latest version of Kamu SM Certificate Policy and Certification Practice Statement (CP/CPS), published at http://depo.kamusm.gov.tr/ilke/ .

2 Contacts

2.1 General Contacts

Kamu Sertifikasyon Merkezi - GEBZE
TÜBİTAK Yerleşkesi, P.K. 74
Gebze 41470 Kocaeli, TURKEY

Kamu Sertifikasyon Merkezi - ANKARA
T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü
Çamlıca Mahallesi, 408. Cad. No:136 C Blok 5. Kat
Yenimahalle/ANKARA, TURKEY

Call Center: 444 5 576
Tel: +90 (0) 262 648 18 18
Fax: +90 (0) 262 648 18 00
E-mail: bilgi@kamusm.gov.tr
Web: http://www.kamusm.gov.tr

2.2 Contact Information for Problem Reporting and Revocation

Call Center: 444 5 576
E-mail: bilgi@kamusm.gov.tr
Web: http://www.kamusm.gov.tr

See section 4.9.3 of the Kamu SM CPS for revocation process.

3 Certificate Type, Validation Procedures and Usages

Kamu SM provides OV SSL certificates in accordance with "Organizational Validation Certificate Policy " defined in ETSI EN 319 411-1 standard. For this end, there is a hierarchy consisting of a root CA at the top and subordinate CAs under it. SSL certificates are issued by subordinate CA. SHA-256 with RSA algorithm (OID = {1 2 840 113549 1 1 11}) is used in signing all certificates issued by Kamu SM.

Kamu SM has put restrictions on TLDs belonging to government agencies since it provides OV SSL services to government agencies. The TLDs to be certified are determined as gov.tr, k12.tr, pol.tr, mil.tr, tsk.tr, kep.tr, bel.tr, edu.tr, org.tr. SSL services are not provided for TLDs outside these.

Content of each certificate issued by Kamu SM contains an OID of relevant certificate policy for the purpose of specifying according what certificate policy that certificate will be used. OIDs used in SSL certificates issued by Kamu SM are CA/Browser Forum OV SSL OID {2.23.140.1.2.2} and Kamu SM OV SSL OID {2.16.792.1.2.1.1.5.7.1.3}.

Kamu SM authenticates organization identity of government agencies having applied for certificate and domain ownership of the agencies. Validation procedures of subscriber are specified in the CPS Section 3.1 and Section 3.2.

4 Reliance Limits

Kamu SM issues OV SSL certificates to only government agencies of Turkey.

Following electronic or manual documents in relation to certificate application and certificate life cycle are archived:

- All information and documents provided during application by subscriber
- Forms received electronically or manually during certificate issuance and revocation applications
- Important correspondence made regarding certificate events
- All issued certificates
- All expired Kamu SM root and subordinate CA certificates
- All published certificate revocation status logs
- Certificate policy document
- Certificate practice statement document
- Certificate management procedures
- Subscriber agreements

Archived data and documents are retained for a period of minimum 7 (seven) years.

5 Liabilities of Subscribers

Inalienable and exclusive rights are provided to the Subscriber to use the certificate. In this context, Subscriber accepts and undertakes the followings;

a. The Subscriber shall agree that all information material to the issuance of a Certificate that the Subscriber provides to Kamu SM in each Application is accurate and complete or Subscriber will take full responsibility if there are any information inaccuracies and any problems caused by the misinformation.
b. In accordance with this agreement, Subscriber shall not transfer the rights and obligations of using the SSL Certificate to another person or organization.
c. The Subscriber shall not apply for any domain name other than the one officially owned by the organization and submitted on the Certificate Application.
d. In order to verify the official organization name and the domain name, the Subscriber shall complete the following steps,
    - Kamu SM requests a change on a page serviced over the domain of the Subscriber in order to verify Subscriber's control over the domain. For this purpose, Subscriber is requested to publish a content named as request token including information about the certificate signing request in a file named as "kamusmdv.txt" located in .well-known/pki-validation/ directory.
    - The request token is the SHA-256 imprint of the related certificate signing request.
    - After the request token is published, Kamu SM verifies the accuracy of the token and validates the domain name ownership.
e. The Subscriber confirms that the related certificate will not be used on the websites which include improper and illegal content.
f. The Subscriber shall generate key pair by itself and shall create Certificate Signing Request (CSR) as to prove that private key belongs to itself. The private key shall not be shared and generated by other third parties. The Subscriber shall take all required measures for protecting the confidentiality and integrity of its private key. In case of loss, disclosure, modification or unauthorized use of the private key, the Subscriber shall immediately notify Kamu SM.
g. The Subscriber shall take all required precautions for protecting the confidentiality and integrity of the passwords used for certificate obtaining process.
h. The Subscriber shall use the certificate in accordance with the requirements set out in the CP/CPS documents. Kamu SM has the rights to make changes over these documents if necessary.
i. The Subscriber confirms not to change any information related to the certificate and the Subscriber shall submit an Operation Tracking Form every year during the validity period of the certificate.
j. In the case where the Subscriber's declared information is modified or no longer valid, the subject shall promptly apply to Kamu SM for revocation of the certificate.
k. In the case where the Subscriber is subject to transfer its domain ownership to an organization, SSL Procuratorship Form, which is published by Kamu SM, has to be submitted in addition to application documents. This form has to be signed by both organizations.
l. The Subscriber shall control the accuracy of the information in the certificate.
m. In case of private key compromise, the subject shall immediately cease the use of SSL certificate.

6 Certificate Status Checking Obligations of Relying Parties

Relying parties are liable for performing validity checks of the certificate provided below before performing any action relating to the certificate:

- Verifying that the certificate is used in compliance with its intended purpose of issuance,
- Checking expiration period of the certificate,
- Checking validity of the certificate via CRL or OCSP service,
- Verifying integrity of revocation status record obtained from CRL or OCSP service by using public key existing within relevant certificates of Kamu SM,
- Verifying authenticity of the certificate using public key existing within subordinate CA certificate of Kamu SM,
- Verifying authenticity of subordinate CA certificate of Kamu SM by using public key existing within root certificate,
- Verifying authenticity of root certificate of Kamu SM by checking certificate hash value,
- Verifying that the subscriber possesses private key corresponding to public key within the certificate.

7 Limited Warranty and Disclaimer/Limitation of Liability

Limitations relating to liabilities of Kamu SM and the parties receiving certificate services are designated in SSL Agreement.

8 Applicable Agreements, CPS, CP

The following information is available in the repository to be accessed publicly:

- Root and subordinate CA certificates of Kamu SM,
- OID list used by Kamu SM,
- Kamu SM CP/CPS documents,
- Agreements, forms, certificate contracts, certification management procedures,
- Updated revocation status records

Kamu SM repository is accessible over http://www.kamusm.gov.tr and http://depo.kamusm.gov.tr.

9 Privacy Policy

Kamu SM maintains privacy of personal/organizational information of the certificate applicants, the subscribers or other participants within the scope of the services provided thereon.

a) Information Treated as Private

Information such as demographic information, address information and phone numbers declared to Kamu SM for use within identification, authentication and certificate management procedures during application is treated as private.

b) Information Not Deemed Private

The information contained in the content of the certificate issued by Kamu SM is not confidential.

c) Responsibility to Protect Private Information

Kamu SM does not request information except required information for issuing certificate from the certificate requesting agency. Kamu SM does not use personal/organizational information so obtained for the purposes other than offering certificate service and does not disclose the same to relying parties and does not keep available the certificate in environments accessible by relying parties without consent of the subscriber.

Required security measures are taken by Kamu SM for blocking unauthorized use and access to information required within certificate life cycle during and after application of the subscribers. Only authorized personnel have access to the information of the subscribers.

d) Notice and Consent to Use Private Information

Kamu SM may disclose the information with relying parties with written consent of the subscriber.

e) Disclosure Pursuant to Judicial or Administrative Process

Kamu SM may disclose the confidential information owned by the subscriber pursuant to judicial or administrative process.

10 Refund Policy

If the subscriber identifies that it fails to use its certificate as a result of audit conducted upon first delivery and it is understood that this issue arises from an error resulting from Kamu SM, fee paid for the certificate by the subscriber is refunded upon request.

11 Applicable Law, Complaints and Dispute Resolution

In the event the provisions contained in CP/CPS document are found to be in contradiction with the relevant legislation to be effective thereafter, required adjustments shall be made and duly adapted. Competent courts will be Gebze Courts, Republic of Turkey in settlement of disputes.

All disputes arising out of the parties will be settled amicably. It shall be referred to the contracts mutually concluded thereon, agreements, the document of Kamu SM Certificate Policy and Kamu SM Certification Practice Statement in settlement of disputes. If disputes fail to be settled amicably, competent courts will be Gebze Courts, Republic of Turkey in settlement of disputes.

12 TSP and Repository Licenses, Trust Marks, and Audit

Whether or not Kamu SM meets the requirements in CP/CPS document shall be audited at least annually. There is no time gap between audits.

Before December 2018, these audits consists of external audits within the scope of ETSI TS 102 042 and CA/B Forum the Baseline Requirements made by Information and Communication Technologies Authority having official audit authority authorized by the law of Republic of Turkey. In line with the updated standards, these audits made by the Qualified Auditor within the scope of ETSI EN 319 411-1 and CA/B Forum the Baseline Requirements since December 2018. Pursuant to Standard ETSI EN 319 411-1, Organization Validated Certificate (OV SSL) processes are subject to audits by an authorized independent auditor.

Information Security Management System audits conducted within the scope of ISO 27001 and internal audits conducted by reliable personnel.

Audit reports are available at http://www.kamusm.gov.tr