PUBLIC

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM SSL PKI DISCLOSURE STATEMENT

Document Code

PRO.01.02

Version No

06

Issue Date

19.12.2023

PUBLIC

DOCUMENT PREPARATION HISTORY		
Version No	**Reason for Release**	**Issue Date**
00	Initial Release	22.10.2018
01	Changes have been made within Contact Information for Problem Reporting and Revocation, added information about Personal Data Protection Law and available information in the repository.	25.10.2019
02	Changes have been made about Operation Tracking Form within the Liabilities of Subscribers part and Reliance Limits part.	15.09.2020
03	Changes have been made due to an update in the Domain Control Validation methods within the Liabilities of Subscribers part.	01.12.2021
04	Retention period of archives has been reduced to minimum 2 (two) years.	07.07.2022
05	Changes have been made due to an update in website link for Personal Data Protection Law.	17.08.2023
06	Updates are done within the scope of issuing SSL certificates for domain names ending with “.tr” ccTLD.	19.12.2023

CONTENTS

1 Goal and Scope

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 Responsibilities

Kamu SM, Subscribers and the relying parties fulfill the representations and warranties mentioned in the certificate contracts and agreements.

2.1 General Contacts

Kamu Sertifikasyon Merkezi - GEBZE
TÜBİTAK Gebze Yerleşkesi (İdari Bina), 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: (+90) 444 5 576 / (+90) 850 460 55 76
Fax: (+90) 262 648 18 00
E-mail: bilgi@kamusm.gov.tr
Web: https://kamusm.bilgem.tubitak.gov.tr

2.2 Contact Information for Problem Reporting and Revocation

Call Center: (+90) 444 5 576
Problem Reporting E-Mail: kamusm.cainfo@tubitak.gov.tr
Revocation E-mail: ssliptal@kamusm.gov.tr
Web: https://kamusm.bilgem.tubitak.gov.tr

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

3 Definitions and Acronyms

3.1 Definitions

i. **Applicant:** A Government Agency that applies for a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber.

ii. **Certificate Revocation List (CRL):** An electronic file that has been generated, signed and published by the CA to disclose the revoked certificates to the public.

iii. **Certification Authority:** An organization that is responsible for the creation, issuance, revocation, and management of Certificates.
defined in ETSI EN 319 411-1 standard.

iv. **Kamu SM:** Government Certification Authority. A unit of TÜBİTAK in BİLGEM providing certification service for the government agencies.

v. **Key Pair:** The Private Key and its associated Public Key.

vi. **Object Identifier (OID):** A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

vii. **Online Certificate Status Protocol (OCSP):** An online certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.

viii. **OV SSL:** SSL certificate issued and maintained pursuant to "Organization Validation Certificate Policy"

ix. **OV SSL:** SSL certificate issued and maintained pursuant to "Organization Validation Certificate Policy" defined in ETSI EN 319 411-1 standard.

x. **Private Key:** The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

xi. **Public Key:** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

xii. **Relying Parties:** Any natural person or legal entity that relies on a Certificate.

xiii. **Repository:** An online database containing publicly-disclosed PKI governance documents (such as Certificate Policy and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

xiv. **Revocation Status Record:** Record wherein revocation information of unexpired certificates is included and relying parties can swiftly and securely access exact certificate revocation time if revoked.

xv. **Root CA Certificate:** Self-signed certificate issued by the Root CA.

xvi. **Root Certification Authority:** Certificate authority formed within Kamu SM, to whom the most authorized signature degree has been given and has signed its own certificate.

xvii. **SSL Certificate/Certificate:** It authenticates the identity of the web server and ensures the integrity and the security of the data that is being transmitted between server and client.

xviii. **Subordinate CA Certificate:** Certificate of the Subordinate CA.

xix. **Subordinate Certification Authority:** Certificate authority formed within Kamu SM, to whom is the authority to sign SSL certificates and its certificate signed by Root CA.

xx. **Subscriber:** A Government Agency to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

xxi. **Working Day:** Weekdays except national holidays and the weekend.

3.2 Acronyms

BR: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted

CA: Certification Authority

ccTLD: Country Code Top-Level Domain

Certificates – CA/Browser Forum Baseline Requirements Document

CP/CPS: Certificate Policy and Certification Practice Statement

CRL: Certificate Revocation List

CSR: Certificate Signing Request

ETSI EN: ETSI European Standard

ETSI TS: ETSI Technical Specifications

ETSI: European Telecommunications Standards Institute

Kamu SM: Government Certification Authority of Turkey

OCSP: Online Certificate Status Protocol

OID: Object Identifier

SSL: Secure Socket Layer

TLD: Top Level Domain

4 Implementations

4.1 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 issues OV SSL certificates to government agencies with domain names ending with ".tr" ccTLD. SSL certificates are not issued for other TLDs.

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. Verification procedures of Subscriber are specified in the CPS Section 3.1 and Section 3.2.

4.2 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 the Subscriber and records of their verification
- Forms received electronically or manually during certificate issuance and revocation applications
- All issued certificates
- All expired Kamu SM root and subordinate CA certificates
- All published certificate revocation status logs
- Certificate Policy and Certification Practice Statement document
- Certificate management procedures
- Subscriber agreements
- NTP synchronization logs of system that used for certification processes.

Archived data and documents are retained for a period of minimum 2 (two) years from their record creation timestamp, or as long as they are required to be retained per laws and/or ETSI standards, whichever is longer.

4.3 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. The Subscriber confirms that the information provided by SSL Application Form can be stored and processed according to Personal Information Privacy Protection Law no.6698.
c. In accordance with this agreement, Subscriber shall not transfer the rights and obligations of using the SSL Certificate to another person or organization.
d. The Subscriber shall not apply for any domain name other than the one officially owned by the organization and submitted on the Certificate Application.
e. In order to verify the control over domain name ownership, the Subscriber shall perform the methods specified in Section 3.2.2.4 of the Kamu SM SSL CP/CPS document. Related document is available on http://depo.kamusm.gov.tr/ilke/ web page.
f. The Subscriber confirms that the related certificate will not be used on the websites which include improper and illegal content.
g. The Subscriber shall Install the certificate only on servers that are accessible at the “Subject Alternative Names” listed in the certificate,
h. 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.
i. The Subscriber shall take all required precautions for protecting the confidentiality and integrity of the passwords used for certificate obtaining process.
j. 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.
k. The Subscriber shall use the certificate solely in compliance with all applicable laws and solely in accordance with Subscriber Agreement,
l. In the case where the Subscriber’s declared information is modified or no longer valid, the Subscriber shall promptly apply to Kamu SM for revocation of the certificate.
m. The Subscriber shall control the accuracy of the information in the certificate.
n. SSL certificate shall be deemed to have been accepted in case of no return within 10 working days following sending it to applicant.
o. In case of private key compromise, the Subscriber shall immediately cease the use of SSL certificate.
p. The Subscriber shall agree that Kamu SM is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the CP/CPS or BRs.

q. The Subscriber shall respond to the Kamu SM's instructions concerning key compromise or certificate misuse within a reasonable time.
r. The Subscriber confirms that the relevant documents and records can be transferred in the case the Kamu SM certificate services are terminated by transferring to another Certificate Authority.

4.4 Certificate Status Checking Obligations of Relying Parties

Relying parties are liable for performing validity checks of the certificate provided below prior to relying on a certificate:

- Have technical capability to use certificates,
- Verify the validity and revocation of the CA and Subscriber certificates using CRL or OCSP,
- Verify that the certificate is used in compliance with its intended purpose of issuance,
- Take account of any limitations on the usage of the certificate either indicated in the certificate or CP/CPs,
- Check expiration period of the certificate,

4.5 Limited Warranty and Disclaimer/Limitation of Liability

Kamu SM shall not be liable to the Subscriber, relying party or any other third parties for any losses suffered as a result of use or reliance on such certificate.

All liability is limited to actual and legally provable damages.

The liability and/or limitation thereof of Subscribers and Kamu SM shall be as set forth in the applicable Subscriber Agreements.

4.6 Applicable Agreements, CPS, CP

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

- Root and subordinate CA certificates of Kamu SM,
- Hash values of certificates of Kamu SM and hash algorithms used in the calculation of hash values,
- OID list used by Kamu SM,
- Up-to-date and older versions of Kamu SM CP/CPS documents,
- Agreements and forms,
- Updated revocation status records

Kamu SM repository is accessible over https://kamusm.bilgem.tubitak.gov.tr and http://depo.kamusm.gov.tr.

4.7 Privacy Policy

Kamu SM maintains privacy of personal/organizational information of the Applicants, the Subscribers or other participants within the scope of the services provided thereon and they are all informed accordance with the law Personal Information Privacy Protection no.6698.

a) Information Treated as Private

Personal 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.

Kamu SM provides information as part of Personal Data Protection Law on its website.

d) Notice and Consent to Use Private Information

Kamu SM may disclose the private information with third parties after obtaining the Subscriber's consent or as required by applicable law or regulation.

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.

4.8 Refund Policy

If the subscriber identifies that it is unable to use its certificate upon first delivery within the period specified in CP/CPS Section 4.4.1 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.

4.9 Applicable Law, Complaints and Dispute Resolution

All related parties including Kamu SM, Subscribers and relying parties agree to comply with applicable laws and regulations as pertaining in Turkish Republic. 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.

All disputes arising out of the parties will be settled amicably. It shall be referred to the contracts mutually concluded thereon, agreements, and the document of Kamu SM Certificate Policy and Certification Practice Statement in settlement of disputes. Before resorting to any dispute resolution mechanism, parties are required to notify Kamu SM and attempt to resolve disputes directly with Kamu SM. If disputes fail to be settled amicably, competent courts will be Gebze Courts, Republic of Turkey in settlement of disputes.

4.10 TSP and Repository Licenses, Trust Marks, and Audit

Audits within the scope of ETSI EN 319 411-1 and CA/B Forum the BRs are made by a qualified auditor on an annual and contiguous basis. An audit period does not exceed one year in duration and the scope of these audits is limited to OV SSL.

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