

PUBLIC



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KAMU SM SSL PKI DISCLOSURE STATEMENT

Document ID

PRO.01.02

Version

10

Date

15.04.2026

PUBLIC

REVISION HISTORY		
Version	Description of Changes	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
07	Editorial adjustments have been made.	26.12.2024
08	Changes have been made within Liabilities of Subscriber regarding the Mass Revocation Event.	08.04.2025
09	Updates are done to extend the scope of OV SSL Certification Service.	19.06.2025
10	Added cross-certification model to the SSL certificate hierarchy and editorial adjustments have been made.	15.04.2026

CONTENTS

1	<i>Goal and Scope</i>	3
2	<i>Responsibilities</i>	3
2.1	General Contacts	3
2.2	Contact Information for Problem Reporting and Revocation	3
3	<i>Definitions and Acronyms</i>	4
3.1	Definitions	4
3.2	Acronyms	5
4	<i>Implementations</i>	6
4.1	Certificate Type, Validation Procedures and Usages	6
4.2	Reliance Limits	6
4.3	Obligations of Subscribers	7
4.4	Certificate Status Checking Obligations of Relying Parties	8
4.5	Limited Warranty and Disclaimer/Limitation of Liability	8
4.6	Applicable Agreements, CPS, CP	9
4.7	Privacy Policy	9
4.8	Refund Policy	10
4.9	Applicable Law, Complaints and Dispute Resolution	10
4.10	TSP and Repository Licenses, Trust Marks, and Audit	10

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, Prof. Dr. Haydar BAŞ 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 legal entity 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 (CA):** An organization that is responsible for the creation, issuance, revocation, and management of Certificates defined in ETSI EN 319 411-1 standard.
- iv. **Cross Certificate:** A certificate that is used to establish a trust relationship between two CAs.
- v. **Kamu SM:** A TÜBİTAK unit providing certification services for organizations located in Turkey.
- vi. **Key Pair:** The Private Key and its associated Public Key.
- vii. **Mass Revocation Event:** The revocation of a substantial number of certificates within a relatively short timeframe due to a common cause, compliance requirement, or security incident.
- viii. **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.
- ix. **Online Certificate Status Protocol (OCSP):** An online certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.
- x. **OV SSL:** SSL certificate issued and maintained pursuant to "Organization Validation Certificate Policy" defined in ETSI EN 319 411-1 standard.
- xi. **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.
- xii. **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.
- xiii. **Relying Parties:** Any natural person or legal entity that relies on a Certificate.
- xiv. **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.
- xv. **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.
- xvi. **Root CA Certificate:** Self-signed certificate issued by the Root CA.
- xvii. **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.
- xviii. **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.
- xix. **Subordinate CA Certificate:** Certificate of the Subordinate CA.

- xx. **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.
- xxi. **Subscriber:** A legal entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
- xxii. **Working Day:** Weekdays except national holidays and the weekend.

3.2 Acronyms

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

CA: Certification Authority

ccTLD: Country Code Top-Level Domain

CP/CPS: Certificate Policy and Certification Practice Statement

CRL: Certificate Revocation List

CSR: Certificate Signing Request

ETSI EN: ETSI European Standard

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 issues OV SSL certificates in accordance with the “Organizational Validation Certificate Policy” defined in ETSI EN 319 411-1.

These certificates are issued to legal entities for the purpose of securing electronic communications (e.g. TLS/SSL) and for authentication of the Subscriber’s identity and domain ownership.

Kamu SM issues OV SSL certificates only to organizations legally established in Turkey and holding domain names under the “.tr” country code top-level domain (ccTLD).

The Kamu SM SSL certificate hierarchy consists of a Root and Subordinate Certification Authorities. Where necessary, cross certificates may be issued to ensure continuity of trust and interoperability.

- **Root Certificate:** Serves as the trust anchor and is used to issue Subordinate CA Certificates.
- **Cross Certificate:** May be used to establish trust relationships between different certification paths, including transition or interoperability scenarios.
- **Subordinate CA Certificate:** Used to issue end-entity certificates.

Kamu SM may utilize cross-certification within its PKI hierarchy to ensure continuity, interoperability, and compatibility of trust services. As a result, certificate validation may rely on different trust paths depending on the relying party’s trust store and configuration.

Each issued certificate contains references to the applicable Certificate Policy via the Certificate Policies extension. The following Object Identifiers (OIDs) are included in the Certificate Policies extension of SSL certificates:

- CA/Browser Forum OV SSL Certificate Policy: 2.23.140.1.2.2
- Kamu SM OV SSL Certificate Policy: 2.16.792.1.2.1.1.5.7.1.3

Subscriber identity and domain ownership are verified in accordance with the procedures defined in the CP/CPS, including but not limited to Section 3.1 and Section 3.2.

Kamu SM issues certificates to organizations upon request and in accordance with its policies; certificates are not issued anonymously or without proper validation.

4.2 Reliance Limits

SSL certificates issued by Kamu SM are intended to be used for authenticating a server to clients and for establishing encrypted communication between the server and the client.

Relying parties are responsible for assessing the suitability of a certificate for their intended use and for verifying its validity, including the certificate chain, revocation status, and applicable trust anchors.

Kamu SM maintains audit logs and archives records related to certificate lifecycle events in accordance with CP/CPS Section 5.4 and Section 5.5.

Registration information and event logs are retained for a minimum period of two (2) years from their creation, or longer if required by applicable laws or relevant standards.

4.3 Obligations of Subscribers

Subscribers are required to comply with the obligations defined in the applicable CP/CPS and Subscriber Agreement. In this context, Subscribers undertake to:

- a) To declare accurate and complete information during certificate application and to take full responsibility if there are any information inaccuracies and any problems caused by the misinformation.
- b) To read the clarification text on the Kamu SM Website regarding the processing of the personal data within the scope of Personal Information Privacy Protection Law no.6698.
- c) Not to transfer the rights and obligations of using the SSL Certificate to another person or organization.
- d) Not to apply for any domain name other than the one officially owned by the organization and submitted on the Certificate Application.
- e) To complete the necessary steps in the domain ownership verification process, in order to verify the officially owned domain names.
- f) Not to be used the SSL certificate on the websites which include improper and illegal content.
- g) Not to be used the SSL certificate on servers and systems that cannot tolerate revocation.
- h) To follow the notification regarding revocation process and act in accordance with the revocation timeline within the periods specified in Section 4.9.1.1 of the Kamu SM SSL CP/CPS document by working in cooperation with the Kamu SM in cases requiring certificate revocation.
- i) To accept the decisions and practices taken in the revocation processes by Kamu SM due to the obligation to comply with international standards.
- j) To generate key pair by itself and 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 the Kamu SM.
- k) To take all required precautions for protecting the confidentiality and integrity of the passwords used for certification process.
- l) To use SSL Certificate as specified in CP/CPS document (Kamu SM has to right to change CP/CPS document when it deems necessary).

- m) To inform Kamu SM, and apply for revocation of the SSL Certificate in case the information declared during the application becomes invalid.
- n) To control the accuracy of the information in the certificate,
- o) To deem have been accepted in case of no return within 10 working days following sending the SSL certificate to the applicant.
- p) To cease the use of SSL certificate in case of private key compromise.
- q) To confirm that the relevant documents and records can be transferred.

4.4 Certificate Status Checking Obligations of Relying Parties

Relying parties are responsible for performing appropriate certificate validation checks prior to relying on a certificate. A relying party may be considered to reasonably rely on a certificate only if the following actions are performed:

- Possess the technical capability to process and validate certificates,
- Verify the validity of the certificate, including the certification path,
- Check the revocation status of both the CA and end-entity certificates using CRLs and/or OCSP,
- Ensure that the certificate is used in accordance with its intended purpose,
- Take into account any limitations on certificate usage as specified in the certificate and the applicable CP/CPS,
- Verify that the certificate is within its validity period (not expired).

Any reliance on a certificate without performing the above checks shall be at the relying party's own risk.

4.5 Limited Warranty and Disclaimer/Limitation of Liability

Kamu SM warrants that it performs its services in accordance with the applicable CP/CPS.

Kamu SM does not guarantee that certificates will be fit for any particular purpose beyond those specified in the applicable CP/CPS.

To the extent permitted by applicable law, Kamu SM shall not be liable for indirect, incidental, or consequential damages arising from the use of, or reliance on, a certificate.

Kamu SM's liability is limited to direct damages that are duly proven in accordance with applicable law.

Further details regarding warranties, disclaimers, and limitations of liability, including those applicable to Subscribers and relying parties, are set forth in the applicable Subscriber Agreements and related contractual documents.

4.6 Applicable Agreements, CPS, CP

The services provided by Kamu SM are governed by the applicable CP/CPS and related agreements, including Subscriber Agreements and other contractual documents.

Kamu SM issues OV SSL certificates in accordance with its Organizational Validation Certificate Policy. The applicable CP/CPS is identified by the following Object Identifier (OID):

- Kamu SM OV SSL Certificate Policy: 2.16.792.1.2.1.1.5.7.1.3

Detailed information on certificate issuance, management, validation, and revocation procedures is provided in the relevant CP/CPS documents.

All applicable documents, including current and previous versions of CP/CPS, agreements, and other relevant information, are made publicly available via the Kamu SM repository:

- <https://kamusm.bilgem.tubitak.gov.tr>
- <http://depo.kamusm.gov.tr/ilke>

4.7 Privacy Policy

Kamu SM maintains confidentiality of personal/organizational information of Applicants, Subscribers, and other participants within the scope of the services it provides. All personal data are processed in accordance with applicable data protection legislation, including the law on the Protection of Personal Data No. 6698.

a) Information Treated as Private

Personal data such as identity information, demographic data, address details and contact information provided to Kamu SM during identification, authentication and certificate lifecycle management processes shall be treated as confidential and processed only for certification service purposes.

b) Information Not Deemed Private

Information contained in the issued certificates, including but not limited to subject name, domain name, and certificate validity information is considered public and may be disclosed via certificates and related services.

c) Responsibility to Protect Private Information

Kamu SM collects only the information necessary for certificate issuance and lifecycle management. Such information shall not be used for purposes other than certification services and shall not be disclosed to unauthorized third parties, including relying parties, except as permitted by applicable laws or with the explicit consent of the Subscriber.

Kamu SM implements appropriate technical and organizational security measures to protect personal data against unauthorized access, disclosure, alteration, and destruction. Access to such information is restricted to authorized personnel on a need-to-know basis.

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

d) Notice and Consent to Use Private Information

Subscribers are informed about data processing activities in accordance with applicable data protection legislation. Where required by law, explicit consent of Subscriber is obtained prior to the processing or disclosure of personal data.

e) Disclosure Pursuant to Judicial or Administrative Process

Kamu SM may disclose confidential information to competent authorities pursuant to judicial or administrative requests in accordance with applicable laws.

f) Data Retention

Registration information and related records are retained for a minimum period of two (2) years, or longer if required by applicable laws or relevant standards.

4.8 Refund Policy

If the subscriber determines that it is unable to use its certificate upon initial delivery, within the period specified in CP/CPS Section 4.4.1 and if it is determined that the issue arises from an error resulting from Kamu SM, the fee paid for the certificate shall be refunded upon Subscriber's 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 BR 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.