SECURE SOCKET LAYER (SSL) CERTIFICATE APPLICATION FORM AND SUBSCRIBER AGREEMENT

Organization Information

Organization Name:	
Address:	
State:	
Tax Office:	
Tax Number:	
Phone:	

Contact Point Information

Contact Point is responsible for operations about SSL certificate life-cycle between Kamu SM and the organization. Contact point is the person who is officially appointed to carry out the process related to the SSL certificate such as application and revocation on behalf of the organization.

Full Name:	
Department:	
Rep. of Turkey ID:	
Corporate E-Mail:	
Office Phone:	

Within the scope of Turkish Personal Data Protection Law no.6698, I have read the information shared on the page "GDPR Information" and accept the processing of my personal data that I have declared in this context. I declare that I am responsible for all issues that may arise if the above-mentioned information is not correct, and I accept that I am responsible for all SSL operations for relevant domain name on behalf of my organization.

(●) This form will be electronically signed by contact point.

This form has to be prepared within ECP 2.0 file together with cover letter and then sent to Kamu SM. The ECP file has to be signed by the contact point and the authorized person in Organization Declaration section. File has also to be sealed using electronic seal of the organization. The prepared ECP file with PKCS#10 certificate signing request file should be sent from the corporate e-mail.

( ) This form will be handwritten signed by contact point.

The prepared form together with the PKCS#10 certificate signing request file, has to be sent bilgi@kamusm.gov.tr via e-mail. The original file has also to be sent to TÜBİTAK BİLGEM, P.K. 74 41470 Gebze Kocaeli by mail.

SECURE SOCKET LAYER (SSL) CERTIFICATE APPLICATION FORM AND SUBSCRIBER AGREEMENT

Technical Information

- In this field, the requested SSL certificate type shall be selected and the domain names to be certified shall be written.
- It should be ensured that the domain name is written correctly and the sample writing format should be taken into account according to the certificate types in table below. Domain ownership verification will be performed by Kamu SM for the domains requested in this section. For detailed information, see Chapter 3: Domain Ownership Verification . Kamu SM will contact with you for selection of the domain verification method.
- All SSL certificates that are issued by Kamu SM are valid for 1 (one) year.

☐ **Standart SSL Certificate**

-The certificate is issued for a single domain name.
-The field should be filled according to the number of certificate request, if not used it should be left blank.

Example writing format:
abc.domain.gov.tr

Domain Names to be certified

☐ **Wildcard SSL Certificate**

-The certificate covers all subdomains of the requested domain name.
-Base domain name will also be covered by certificate.
-The field should be filled according to the number of certificate request, if not used it should be left blank.

Example writing format:
*.domain.gov.tr

Domain Names to be certified
*.
*.
*.
*.
*.

☐ **SAN SSL Certificate**

- The certificate covers multiple domains with a single certificate.
- In the first line at the top, the domain name appear in the "Common Name (CN)" field of the certificate should be written.
-At the bottom, the domain names that appear in "SAN" field of the certificate should be written.

Example writing format:
abc.domain.gov.tr
www.domain.gov.tr
info.testdomain.gov.tr

Domain Names to be certified

1. Definitions and Abbreviations

SSL Certificate: It authenticates the identity of the web server and it ensures the integrity and the security of the data that is being transmitted between server and client.
OV SSL: It is an organization-validated SSL certificate that contains information about the organization in addition to domain name.
Subscriber: A government organization requesting SSL certificate and having the control over domain name in the requested certificate.
Domain Name: It corresponds to the names instead of IP addresses that are used to identify the servers of institutions and brands that serve on the internet.
Key Pair: The Private Key and its associated Public Key.
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.
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.
Kamu SM: Government Certification Authority. A unit of TÜBİTAK in BİLGEM providing certification service for the government agencies.
CP (Certificate Policies): A document which includes the necessary set of rules for the creation/implementation of the SSL Certificate and the Public Key Infrastructure architecture to meet the security requirements.
CPS (Certificate Practice Statements): A document which defines the roles, responsibilities, and relationships of system entities and also describes the realization method of registration and certification management procedures for SSL certificate.
ECP (E-Correspondence Project): The project has been launched with purpose of ensuring that official correspondence between public institutions and organizations is carried out in a secure electronic environment.

2. Preparation of PKCS#10 Certificate Signing Request

In order to issue SSL certificate, a certificate signing request (CSR) shall be created by the organization in PKCS#10 format. The required and forbidden fields in the Subject of a CSR are given below.

- It is recommmended that all fields except Common Name (CN) be capitalized.
- Turkish characters shall not be used when filling the fields in the PKCS#10 file.

Subject	Status	Explanations
CN (CommonName)	Required	Name of server registered on behalf of the subscriber government agency in DNS is written in “CN” field. "*.<domain name>" is written in this field in OV SSL wildcard certificates. Example: *.testdomain.gov.tr This field does not contain non-distinctive names such as “*.com” or “*.com.tr". IP address or internal server name is not written in this field.
O (Organization)	Required	“O (Organization)” field contains the open title or understandably abbreviated form of subscriber government agency as laid down in organizational law or other legislation. The information is written in this field shall be exactly the same as the "Organization Name" field in this form.
C (Country)	Required	"C (Country)” field includes country code (TR) contained in ISO 3166-1 Alpha-2 standard of the country where subscriber government agency is located.
ST (State or Province)	Required	"ST (State or Province)” field contains province information where subscriber government agency is located.
OU (Organizational Unit) L (Locality) emailAddress givenName surName		Should not be used.

3. Domain Ownership Verification

Before the issuance of the certificate, the ownership of the domain name for which the certificate is requested shall be verified. At this point, two different methods are offered by Kamu SM to verify domain ownership. One of the methods listed below can be preferred.

3.1. Constructed E-Mail to Domain Contact:

- In this method, it is necessary to have a mail server related to the domain name to be certified.
- Kamu SM sends an e-mail including a random value to one of the e-mail addresses of the DNS mail server (admin@domainname, administrator@domainname, webmaster@domainname, hostmaster@domainname, postmaster@domainname).
- The applicant forwards the e-mail including random value back to Kamu SM.
- Kamu SM checks the received random value. If sent and received values are the same then domain ownership is verified.

3.2. DNS Change:

- In this method, the DNS record shall be changed by accessing the control panel of the domain name to be certified.
- Kamu SM sends the random value to corporate e-mail of the contact point.
- The applicant creates a DNS TXT or CNAME record using the random value specified by Kamu SM. You can see the guide to create DNS record on Kamu SM web site.
- Kamu SM checks the presence of the random value in DNS record and domain ownership is verified.

4. Explanations

- Kamu SM has put restrictions on TLDs belonging to government agencies since it provides OV SSL sservices only 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 except these.
- This application form is prepared for organizations in order to declare the server to be certified with written format, and for sending it to Kamu SM.
- Before filling out this form, it should be ensured that it is the current version published on the Kamu SM website, should be read carefully and filled completely. Organization approval fields have to be sealed and signed. If the seal is not available, stamp can also be used. In case of any missing field in the form, certificate issuance would not be possible.
- Domain names to be certified should be written to appropriate section in technical information field (web sites that requested SSL certificate shall have this/these name(s)).
- The applicant shall also be the owner of the domain name.
- Contact point is a person who carries out the operations about SSL certificate between Kamu SM and the organization.
- The application form and its cover letter should be prepared as/within ECP 2.0 file and then sent to Kamu SM. The ECP file has to be signed by the contact point and the authorized person mentioned in Organization Declaration section. File has also to be sealed using electronic seal of the organization. The prepared ECP file together with PKCS#10 certificate request file should be sent from the corporate e-mail.
- In the case of the organizations cannot create ECP 2.0 file, the printed version of the form shall be approved with handwritten signature of the contact point and authorized person mentioned in Organization Declaration section. The prepared form together with the PKCS#10 certificate signing request file, has to be sent bilgi@kamusm.gov.tr via e-mail. After the prepared documents are sent to bilgi@kamusm.gov.tr via e-mail, the original file should also be sent to “TÜBİTAK BİLGEM, P.K. 74 41470 Gebze Kocaeli” address by mail.
- If the information declared in application form and subscriber agreement does not match with CSR file, application will not be processed. In this case, Kamu SM will not be responsible for any problems that may occur.
- If there is no problem in the application documents, the certificate will be issued and sent to the corporate e-mail of the contact point.
- It is the responsibility of the organization to upload the certificate to the server, and in case of deletion or loss of private key for various reasons certificate is reissued for a fee.

- The private key to be used in the SSL certificate application is generated by the applicant and this key shall be at least RSA 2048 bits long. Private key information should never be shared with Kamu SM.
- Kamu SM issues SSL certificates compatible with Certificate Transparency project. Therefore issued certificates are logged to publicly available log servers.
- The validity period of issued certificates will be 1 year (365 days).

5. Revocation of SSL Certificate

Certificate revocation request can only be submitted by the Subscriber. Kamu SM revokes the related certificate upon this request. In case of such a situation, the Subscriber does not have the right to demand a refund for the revoked certificate. Kamu SM reserves the right to revoke certificate in the following cases by notifying the Subscriber.:

a. Considering the subscriber has not fulfill the requirements stated in the SSL Agreement.
b. Considering a misuse of the certificate with the requirements stated in the SSL Agreement and CP/CPS document.
c. Compromise of the Kamu SM systems as mentioned in CP/CPS or the termination of certificate services.
d. The emergence of the other situations as mentioned in CP/CPS which require certificate revocation.

6. Duration of Agreement

The agreement starts when it is signed by the Subscriber and afterward the Subscriber commits that it had read and accepted all the terms and conditions of this agreement and is legally bound by the relevant Terms and Conditions. The expiration date of agreement is limited with the validity of the Certificate. The issue and expiration date of the Certificate will be indicated in the Certificate.

7. Termination of Agreement

If the organization does not fulfill any of its debts, obligations and commitments arising and/or will arise from this Commitment on time, or fails to fulfill its obligations, the services offered by TÜBİTAK BİLGEM by notifying the institution may be stopped and the agreement may be terminated immediately without any liability for compensation. TÜBİTAK BİLGEM has the right to terminate this agreement without giving any reason, by notifying the organization.

8. Terms and Conditions

8.1. Policy Being Applied

Kamu SM executes its operations in conformance with Kamu SM SSL CPS document while providing Organization Validated SSL (OV SSL) certificate. This document determines practice responsibilities of Kamu SM, subscribers and relying parties.

Kamu SM conforms to updated versions of the standard of “ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements” and “CA/ Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates” published on https://www.cabforum.org while providing certification services. In the event of any inconsistency between the CPS document and these documents, the requirements set out in respective documents take precedence over Kamu SM SSL CPS document.

Kamu SM repository is accessible over http://depo.kamusm.gov.tr and http://depo.kamusm.gov.tr/ilke. The SSL Application Form and Subscriber Agreement, CP and CPS documents and all the Root and Subroot Certificates are internationally 24/7 available through Kamu SM repository.

8.2. Usage Limitations

Kamu SM has put restrictions on TLDs belonging to government agencies since it provides OV SSL services only 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 except these. All SSL certificates that are issued by Kamu SM are valid for 1 (one) year.

8.3. Subscriber Obligations and Liabilities

The certificate provides the owner with a non-transferable and exclusive right of use. Subscriber represents and warranties,

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 confirm that the information provided by SSL Application Form can be stored and processed according to 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) 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 Kamu SM.
h) To take all required precautions for protecting the confidentiality and integrity of the passwords used for certification process.
i) To use SSL Certificate as specified in CP and CPS documents (Kamu SM has to right to change CP/CPS documents when it deems necessary).
j) To inform Kamu SM, and apply for revocation of the SSL Certificate in case the information declared during the application becomes invalid.
k) To control the accuracy of the information in the certificate,
l) To deem have been accepted in case of no return within 10 working days following sending the SSL certificate to the applicant.
m) To cease the use of SSL certificate in case of private key compromise.
n) To confirm 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.

8.4. Relying Parties

Public key contained within the certificate of the subscriber may be used for verification purposes by relying parties. Relying parties shall be liable for checking the validity of CA certificate issuing the certificate and the certificate itself, for verifying that the certificate is used in line with the purposes specified in the “Key Usage” field and for conforming to use terms specified in CP/CPS.

If the certificate validation is unsuccessful, the procedure should not be performed based on the certificate. Kamu SM shall not be responsible for a failure of relying parties to fulfill the said requirements thereon in use of public key and certificate.

8.5. Retention Period of Logs

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,
- CP/CPS document,
- Certificate management procedures,
- Subscriber agreements and
- NTP (Network Time Protocol) synchronization logs of system that used for certification processes.

Archived data and documents are retained for a period of minimum 2 (two) years.

8.6. Resolution of Disputes and Complaint Procedure

All disputes arising out of the parties will be settled amicably. It shall be referred to the contracts mutually concluded thereon, agreements, Kamu SM Certificate Policy and Kamu SM 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, the Republic of Turkey in settlement of disputes.

Kamu SM applies a customer complaint procedure in order to evaluate and resolve customer complaints. The relevant procedure document can accessed over Kamu SM web page.

8.7. Certificate Usage

Subscriber shall use its certificate and private key within the framework specified in this document and in CP/CPS document with other regulations and standards being subjected to.

Subscriber shall be liable for protecting its private key against unauthorized access. Private key corresponding to SSL certificate may only be used within the purposes specified in the “Key Usage” field of the certificate.

Kamu SM issues SSL certificates compatible with the Certificate Transparency (CT). Therefore it logs the certificates to CT servers open to public. Kamu SM SSL Root Certificate is included in the trusted root store of Windows, Mac OS 10.14.2+, IOS 12.1.1+, Linux Ubuntu, Pardus (Debian 17.2+) and Android 8.1+ in the browsers like Mozilla Firefox (v56.0+), Google Chrome, Internet Explorer, Microsoft Edge, Opera, Yandex.

8.8. Contact Information

Address :	Kamu Sertifikasyon Merkezi, TÜBİTAK Yerleşkesi P.K. 74, 41470 Gebze-Kocaeli
Phone :	(+90) 444 5 576
Fax :	(+90 (262) 648 18 00
E-Mail :	bilgi@kamusm.gov.tr
Problem Reporting E-Mail:	kamusm.cainfo@tubitak.gov.tr
URL :	https://kamusm.bilgem.tubitak.gov.tr

Organization Declaration

The person whose name, surname and contact information is given in this agreement has been authorized as Contact Point in SSL certificate operations in line with the need of our organization. I accept, declare and agree that the SSL certificate operations will be carried out in accordance with specified in this agreement and Kamu SM SSL CP/CPS documents, and that our organization is responsible to TÜBİTAK BİLGEM for all damages that may arise in case of violation of this agreement.

◉ This form will be electronically signed by contact point.

This form has to be prepared within ECP 2.0 file together with cover letter and then sent to Kamu SM. The ECP file has to be signed by the contact point and the authorized person mentioned in this section. File has also to be sealed using electronic seal of the organization. The prepared ECP file with PKCS#10 certificate request file should be sent from the corporate e-mail.

○ This form will be handwritten signed by contact point.

The prepared form together with the PKCS#10 certificate signing request file, has to be sent bilgi@kamusm.gov.tr via e-mail. The original file has also to be sent to TÜBİTAK BİLGEM, P.K. 74 41470 Gebze Kocaeli by mail.