KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SUBSCRIBER AGREEMENT

This document (here in after referred to as “Agreement”) identifies rights of usage entitled for .....organization (here in after referred to as “Subscriber”) residing at..... for the SSL Certificate issued by “Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (TÜBİTAK BİLGEM)” residing at “Barış Mahallesi, Anibal Caddesi P.K.74, TÜBİTAK Gebze Yerleşkesi 41470 Gebze, Kocaeli”.

This agreement shall be signed by the subscriber and shall be sent to TÜBİTAK BİLGEM together with the SSL Application Form. The agreement enters into effect from the date of the signature and Subscriber accepts that all the terms and conditions of this agreement have been read and the Subscriber is legally bound by the relevant terms and conditions.

1 Definitions and Abbreviations

i. **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.
ii. **Subscriber:** A government organization requesting SSL certificate and having the control over domain name in the requested certificate.
iii. **Domain Name:** It corresponds to IP addresses of servers in service on the internet, and they are identified with corporate identities or trade names.
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. **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.
vii. **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.
viii. **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.
ix. **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.

All Rights are reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by Kamu SM.

2 Subscriber's Liabilities

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.

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 official organization name and the domain name, the Subscriber shall complete the following steps,

   - Kamu SM requests that http(s)://ornek.gov.tr/.wel-known/pki-validation/kamusmdv.txt file path be created on the web page where the SSL certificate is requested, and the hash value of the PKCS#10 SSL certificate signing request be placed in this file for the verification of the officially owned institution name and domain names.
   - The SHA256 hash value of the PKCS#10 certificate signing request shall be calculated using the Kaşif application of Kamu SM which can be downloaded from https://kasif.kamusm.gov.tr.
   - After this hash value is placed in the relevant file and published, Kamu SM verifies the accuracy of the hash value and validates the domain name ownership.

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 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.

All Rights are reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by Kamu SM.

h. The Subscriber shall take all required precautions for protecting the confidentiality and integrity of the passwords used for certificate obtaining process.
i. The Subscriber shall 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. In case the notified information becomes invalid, the Subscriber informs Kamu SM, and applies for revocation of the SSL Certificate received on behalf of the Subscriber.
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. SSL certificate shall be deemed to have been accepted in case of no return within 10 working days following sending it to the applicant.
n. In case of private key compromise, the subject shall immediately cease the use of SSL certificate.
o. 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.

3 Revocation

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.

The Subscriber Certificate is revoked by the Kamu SM in the following cases and the Subscriber is notified;

a. Considering a misuse of the certificate with the requirements stated in the SSL Agreement and CP/CPS document,
b. Compromise of the Kamu SM system as mentioned in CP/CPS or the termination of certificate services,
c. The emergence of the other situations as mentioned in CP/CPS which require certificate revocation.

4 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.

All Rights are reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by Kamu SM.

5 Termination of Agreement

If the institution 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 KAMU SM by notifying the institution may be stopped and the Undertaking may be terminated immediately without any liability for compensation. KAMU SM has the right to terminate this Undertaking without giving any reason, by notifying the institution.

6 Resolution of Disputes

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.

All Rights are reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by Kamu SM.