KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SERVICE REPRESENTATIONS AND LIABILITIES

1 Definitions and Abbreviations

i. **SSL Certificate/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.

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 the names instead of IP addresses that are used to identify the servers of institutions and brands that serve on the internet.

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

v. **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.

vi. **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.

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

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.

2 Kamu SM's Liabilities

1. Kamu SM manages the SSL certificate lifecycle process in accordance with its CP and CPS documents.
2. 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.
3. Up-to-date versions of CP and CPS documents are 24/7 available through Kamu SM repository.
4. Older versions of CP and CPS documents are available through Kamu SM official web site.
5. All the Root and Subordinate Certificates are 24/7 available through Kamu SM repository.
6. Identification and authentication processes are performed as defined in Kamu SM CPS document.
7. Kamu SM issues SSL certificates compatible with the Certificate Transparency (CT). Therefore it logs the certificates to CT servers open to public.
8. Kamu SM does not use the personal information that belongs to the subject for any purpose except the certificate service provision. Kamu SM takes any measures in order to protect the privacy of such

information according to Personal Information Privacy Protection Law No. 6698 and does not share this information with the third parties without the written consent of the owner or a court decision.

9. Certificate revocation request can only be submitted by the Subscriber. Kamu SM reserves the right to revoke the Subcscriber Certificate in the following cases by notifying the Subscriber;

   - Subscriber not to fulfill the specified requirements in the SSL Agreement,
   - Considering a misuse of the certificate with the requirements stated in the SSL Agreement and CP/CPS document,
   - Compromise of the Kamu SM system as mentioned in CP/CPS or the termination of certificate services,
   - The emergence of the other situations as mentioned in CP/CPS which require certificate revocation.

10. Kamu SM publishes the Certificate Revocation List for the revoked certificates.

11. Kamu SM is not responsible for the Subscriber's misuse of the private key and certificate which occurs in contradiction to related requirements.

12. 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 listed below:

   - Mozilla Firefox (v56.0+),
   - Google Chrome,
   - Internet Explorer,
   - Microsoft Edge,
   - Opera,
   - Yandex.

13. 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 document,
   - 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.