PUBLIC

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

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

Document Code
FRM.01.28

Version No
00

Issue/Revision Date
22.10.2018

PUBLIC

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

DOCUMENT PREPARATION HISTORY		
Version No	**Reason for Release**	**Issue Date**
00	Initial Release	22.10.2018

CONTENTS

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 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.

2 Kamu SM's Liabilities

1. Kamu SM manages the SSL certificate lifecycle process in accordance with its CP and CPS documents.
2. Up-to-date versions of CP and CPS documents are 24/7 available through Kamu SM official web site.
3. All the Root and Subordinate Certificates are 24/7 available through Kamu SM official web site.
4. Identification and authentication processes are performed as defined in Kamu SM CPS document.
5. Kamu SM issues certificates compatible with the certificate transparency. Therefore it has to record certificates in log servers open to public.
6. 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 and does not share this information with the third parties without the written consent of the owner or a court decision.
7. 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;
   - 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.
8. Kamu SM publishes the Certificate Revocation List for the revoked certificates.
9. Kamu SM is not responsible for the Subscriber's misuse of the private key and certificate which occurs in contradiction to related requirements.
10. Kamu SM SSL Root Certificate is included in the trusted root store of Internet Explorer and Mozilla Firefox browsers and for the Microsoft based operating systems, it is in the trusted list of Yandex, Chrome and Opera browsers.
11. In the Android operating system, Kamu SM Root Certificate is trusted by Firefox browser.
12. Kamu SM SSL Root certificate is not trusted yet in browsers running on an Android version older than 8.1 and all versions of IOS operating system.

13. All information and documents provided during application by Subscriber such as:

- 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
- Certificate policy document
- Certificate practice statement document
- Certificate management procedures
- Subscriber agreements

are archived by Kamu SM and these archived data and documents are retained for a period of minimum 7 (seven) years.