

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 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 services.
- viii. **CP/CPS (Certificate Policies and Certificate Practice Statements):** A document which defines rule sets for establishment and implementation of SSL certificate and public key infrastructure architecture in a manner that ensures adherence to security requirements and how these rule sets are to be applied in detail.
- ix. **CRL:** Certificate Revocation List.
- x. **OCSP:** Online Certificate Status Protocol.

2 Kamu SM's Liabilities

1. Kamu SM manages the SSL certificate lifecycle process in accordance with its CP/CPS document.
2. Kamu SM conforms to the current version of the "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 TLS Certificates" published on <https://www.cabforum.org> while providing certification services.
3. Up-to-date versions of CP/CPS documents are 24/7 available through public access repository.
4. Older versions of CP/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 CP/CPS document.
7. Verifies the ownership of the domain names requested in the certificate application as defined in Kamu SM CP/CPS document.
8. Kamu SM issues SSL certificates compatible with the Certificate Transparency (CT). Therefore, it logs the certificates to CT servers open to public.

9. 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.
10. Kamu SM accepts certificate revocation applications in accordance with the procedures specified in CP/CPS and revoke the certificate for any reasons specified in CP/CPS.
11. Kamu SM publishes revoked certificates information in CRL and announce the same via OCSP service.
12. Kamu SM is not responsible for the Subscriber's misuse of the private key and certificate which occurs in contradiction to related requirements.
13. Issued SSL certificates are considered secure by Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, Yandex, Opera, Safari and 360 Browsers running on Android, iOS, Mac OS, Windows and Linux operating systems.
14. Following electronic or manual documents in relation to certificate application and certificate life cycle are archived:
 - All information and documents provided during application by the Subscriber and records of their verification,
 - Forms received electronically or manually during certificate issuance and revocation applications,
 - All issued certificates,
 - All expired Kamu SM root and subordinate CA certificates,
 - All published certificate revocation status logs,
 - Certificate Policy and Certification Practice Statement document,
 - Certificate management procedures,
 - Subscriber agreements,
 - NTP synchronization logs of systems that used for certification processes.

Archived documents are retained for a period of minimum 2 (two) years from their record creation timestamp, or as long as they are required to be retained per laws and/or ETSI standards, whichever is longer.