PUBLIC

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM SSL CERTIFICATE POLICY

Version
v.1.0.1
Issue Date
16.10.2019

PUBLIC

Copyright Notice

Kamu Sertifikasyon Merkezi
TÜBİTAK Yerleşkesi, P.K. 74
Gebze 41470 Kocaeli, TURKEY
http://www.kamusm.gov.tr

TABLE OF CONTENTS

1. INTRODUCTION

Kamu SM (Government Certification Authority) was founded in accordance with Electronic Signature Law no. 5070 dated January 15th, 2004 by The Scientific and Technological Research Council of Turkey (TÜBİTAK). Kamu SM is a government-owned Certificate Authority (CA) operated in compliance with the international standards.

Referred as Certificate Policy (CP), this document has been prepared in compliance with the guide book of "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" for the purpose of describing the rules and working principles to be followed by Kamu SM during providing OV SSL (Organization Validated SSL) certificate to government agencies of Republic of Turkey.

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" referenced in ETSI EN 319 411-1 standard and published on https://www.cabforum.org while providing certification services. In the event of any inconsistency between CP document and these documents, the requirements set out in respective documents take precedence over this document.

This CP document describes execution of the services in regard to accepting certificate applications, certificate issuance and management, certificate revocation procedures in compliance with administrative, technical and legal requirements. This document determines practice responsibilities of Kamu SM, subscribers and relying parties. The certificates issued within this context shall not be considered within the scope of qualified electronic certificate mentioned in Electronic Signature Law no. 5070.

1.1. OVERVIEW

CP document defines the roles, responsibilities and relationships of system entities and also describes method of registration and certification management procedures.

Registration procedures consist of the processes such as receiving applications, identification information, and relevant official documents of government agencies to be certified, verifying and approving such information, receiving and evaluating certificate production and revocation requests, and initiating required procedures in line with approved certificate application and revocation requests.

Certificate management consists of the processes such as generating certificate for subscribers, publishing and revoking certificates, publishing revocation status records, informing relevant parties involved with certification procedures regarding application and certification status and keeping required records.

CP document has been prepared by taking "IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)" as a reference.

1.2. DOCUMENT NAME AND IDENTIFICATION

Document Name: Kamu SM SSL Certificate Policy

Document Version Number: 1.0.1

Date	Changes	Version
07.08.2018	Initial Release	1.0.0
16.10.2019	Updates within the scope of annual CPS revision.	1.0.1

Published on: 16.10.2019

OID: 2.16.792.1.2.1.1.5.7.1.3

This CP document defines the procedures applied by Kamu SM while providing OV SSL certification services and covers OV SSL certificates issued to the servers. OV SSL certificates are issued and managed in accordance with "Organizational Validation Certificate Policy " defined in ETSI EN 319 411-1 standard.

CP document is publicly accessible at http://depo.kamusm.gov.tr/ilke.

1.3. PKI PARTICIPANTS

PKI Participants defined within the scope of this document are the parties bearing relevant rights and obligations within certification services of Kamu SM. These parties are defined as CA, registration authority, subscribers and relying parties. Kamu SM CA activities are all carried out by Kamu SM personnel.

1.3.1. Certification Authorities

Kamu SM provides OV SSL certification service as a CA. Kamu SM OV SSL hierarchy consist of a root CA at the top, a subordinate CA and an OCSP certificate under it; SSL certificates and an OCSP certificate issued by subordinate CA. The subordinate CA fulfil the following services:

- Generating and signing certificates and delivering them to relevant government agencies
- Revoking certificates
- Publication of certificate status information in the form of Certificate Revocation List (CRL) or other methods

1.3.2. Registration Authorities

All registration procedures are directly executed by Kamu SM personnel. Registration units execute services such as certificate application and revocation intended for end users. This unit creates the first customer record and executes required identification and authentication processes and directs relevant certificate requests to certificate generation unit.

1.3.3. Subscribers

Government agencies whose certificates are issued by Kamu SM and which are responsible for using their certificates in compliance with certificate policies and practice statements.

1.3.4. Relying Parties

The parties accepting the certificates by validating them and performing procedures accordingly.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

SSL certificate is used for the purpose of performing authentication between the server and clients, and providing encrypted communication. SSL certificate is deployed only on the server offering service to domain name contained in the certificate. Usage rights of certificates rest with only subscribers.

1.4.2. Prohibited Certificate Uses

SSL certificates issued by Kamu SM may not be used other than the purposes laid down in Section 1.4.1.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CPS document has been written by Kamu SM. Kamu SM may make amendments in the document when it deems necessary.

1.5.2. Contact Person

Questions relating to implementation of this CP document and relevant management policy can be directed to the following contact information of Kamu SM:

Address : Kamu Sertifikasyon Merkezi, TÜBİTAK Yerleşkesi P.K. 74, 41470 Gebze-Kocaeli

Tel **:** 444 5 576

Fax **:** (262) 648 18 00

E-Posta **:** bilgi@kamusm.gov.tr

URL **:** http://www.kamusm.gov.tr

Kamu SM publishes CP document publicly accessible at http://depo.kamusm.gov.tr/ilke.

1.5.3. Person Determining CP Suitability for the Policy

Suitability of CPS to CP document shall be determined by Kamu SM administration and the people authorized by administration.

1.5.4. CPS Approval Procedure

Approval of this CP/CPS documents for publication shall be granted as a result of examinations conducted by Kamu SM administration and the people authorized by administration.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

Certificate Revocation List (CRL): An electronic file that has been generated, signed and published by the CA to disclose the revoked certificates to the public.

Delegated Third Party: A natural person or Legal Entity that is authorized by Kamu SM to assist in the Certificate Management Process by performing or fulfilling one or more of the requirements found herein.

End users: Subscribers and relying parties using the certificates.

Kamu Sertifikasyon Merkezi (Kamu SM): A TÜBİTAK unit providing certification service for the government agencies.

Key pair: Private key and corresponding public key used for creating and verifying electronic signature or encrypting and decrypting data.

Object identification number (OID): Number obtained from an organization identifying an international standard uniquely defining an object.

Online Certificate Status Protocol (OCSP): Standard protocol that has been created to disclose the validity status of certificates to the public, and allows receipt of certificate status information by on-line methods instantly and without interruption.

OV SSL: SSL certificate issued and maintained pursuant to “Organization Validation Certificate Policy” defined in ETSI EN 319 411 standard.

Relying parties: Natural and legal people performing transaction by relying on certificates.

Repository: Data storage medium such as web servers where certificates, revocation status records and certificate procedures and other relevant information are published.

Revocation status record: Record wherein revocation information of unexpired certificates is included and relying parties can swiftly and securely access exact certificate revocation time if revoked.

Root CA Certificate: Certificate of the root CA.

Root Certificate Authority: Certificate authority formed within Kamu SM, to whom the most authorized signature degree has been given and having signed its own certificate.

Subordinate CA Certificate: Certificate of the subordinate CA.

Subordinate Certificate Authority: Certificate authority formed within Kamu SM, to whom the most authorized signature degree has been given and having signed its own certificate.

Subscriber: Government agency obtaining certificate from Kamu SM.

1.6.2. Acronyms

BR: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – CA/Browser Forum Basic Requirements Document

CA: Certificate Authority

CEN: European Committee for Standardization

CP: Certificate Policy

CPS: Certificate Practise Statement

CRL: Certificate Revocation List

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standards Institute

ETSI EN: ETSI European Standard

IETF RFC: Internet Engineering Task Force Request for Comments

ISO/IEC: International Organization for Standardization/International Electrotechnical Committee

Kamu SM: Government Certification Authority of Turkey

OCSP: Online Certificate Status Protocol

OID: Object identification number

PKI: Public Key Infrastructure

SSL: Secure Socket Layer

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Repository is the environment wherein the documents such as root and subordinate CA certificates of Kamu SM, revocation status records, CP and CPS are published uninterruptedly, securely and freely. Some critical files published in repository are updated when necessary. These updates are specified with version numbers and updating date kept on the updated files.

2.1. REPOSITORIES

Kamu SM repository is accessed over the Internet. Kamu SM does not employ a trusted third party to operate the repository.

2.2. PUBLICATION OF INFORMATION

The following information except for those related with internal operations is available in the repository to be accessed publicly:

- Root and subordinate CA certificates of Kamu SM,
- Hash values of certificates of Kamu SM and hash algorithms used in calculation of hash values,
- OID list used by Kamu SM,
- Kamu SM CP and CPS documents,
- Agreements, forms, certificate contracts, certification management procedures,

- Updated revocation status records

Kamu SM repository is accessible over http://www.kamusm.gov.tr and http://depo.kamusm.gov.tr.

2.3. TIME OR FREQUENCY OF PUBLICATION

Agreements, forms, certificate contracts, certification management procedures and CP/CPS documents are updated when their content is modified. Updated documents are promptly published after update.

Certificates of Kamu SM are promptly published after update.

Publication frequency of CRLs and frequency of updating OCSP records are specified in Sections 4.9.7 and 4.9.9. Kamu SM CPS document is regularly updated annually.

2.4. ACCESS CONTROLS ON REPOSITORIES

Kamu SM repository is publicly accessible for acquiring information. Updating repository is carried out by authorized Kamu SM personnel.

Kamu SM fulfils the following representations and warranties in regard to repository:

- Maintaining integrity of the information kept in repository against unauthorized deletion and modification,
- Providing accuracy and up-to-dateless of the information kept in repository,
- Keeping repository accessible at all times,
- Adopting required measures for providing uninterruptible accessibility of repository,
- Providing free access to repository.

3. IDENTIFICATION AND AUTHENTICATION

Kamu SM authenticates organization identity of government agencies having applied for certificate and domain ownership of the agencies. Kamu SM conducts authentication procedures based on all documents and official resources deemed necessary in line with legal and technical requirements.

3.1. NAMING

Identification information of subscriber in the certificates issued by Kamu SM is specified in the CPS document as defined in Section 3.1.

3.2. INITIAL IDENTITY VALIDATION

If applied for the first time for certificate services, the methods defined in the CPS document Section 3.2 shall be applied by Kamu SM to identify relevant agency.

Name or title of government agency to be included on OV SSL certificate shall be verified depending on legal documents. Verification procedure conducted herein shall be executed as designated in Kamu SM procedures.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Certificate re-key is not performed for SSL certificates. If the agency wants, certificate applications are applied like a first time application. In this case, identification and authentication procedures are applied as described in the CPS document Section 3.2.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

In case of a revocation request, Kamu SM calls the agency from the numbers registered in its system, identifies and authenticates the requester and confirms the revocation request.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This part describes the procedures performed in certification management processes. Details relating to the processes are revealed on web site of Kamu SM.

4.1. CERTIFICATE APPLICATION

Who can submit a certificate application and responsibilities of government agency having applied for SSL certificate is defined in the CPS document Section 4.1.

4.2. CERTIFICATE APPLICATION PROCESSING

SSL applications shall be executed in pursuance of the principles set out in Section 3.2 and 4.1 and the procedures of Kamu SM in parallel with this. Approval or rejection of certificate applications and time to process certificate applications are defined in the CPS document Section 4.2.

4.3. CERTIFICATE ISSUANCE

Certificate applications accepted in pursuance of the principles contained in the CPS document Section 4.2.2 shall be processed by Kamu SM and certificate shall be issued following verification of CSR file. All the steps during this procedure are logged.

Kamu SM shall send the certificate to organization representative’s verified e-mail address.

4.4. CERTIFICATE ACCEPTANCE

Subscriber shall check whether or not the information contained in certificate is identical to the information it has declared during application and in case of any inconsistency, it shall immediately notify Kamu SM and shall not use the certificate. In this case, the certificate shall be revoked by Kamu SM.

All SSL certificates issued by Kamu SM are logged to Certificate Transparency servers.

4.5. KEY PAIR AND CERTIFICATE USAGE

Regulations on the use of certificates and private keys by subscribers and relying parties are defined in the CPS document Section 4.5.

4.6. CERTIFICATE RENEWAL

Certificate renewal refers to renewal of the certificate by using the same key pair. Kamu SM does not perform certificate renewal for SSL certificates. In the event the subscriber wants to make a renewal application, it is considered as a new certificate application stated in the CPS document Section 4.1.

4.7. CERTIFICATE RE-KEY

Certificate re-key refers to issuing a new certificate to replace the current certificate without making any modification except the key pair before the expiry date. Kamu SM does not perform certificate re-key for SSL certificates. In the event the subscriber wants to make a re-key application, it is considered as a new certificate application stated in the CPS document Section 4.1.

4.8. CERTIFICATE MODIFICATION

In case of modification within the information in the content of a certificate issued by Kamu SM, the certificate shall be revoked and an application shall be made for a new certificate together with new information. In the event the subscriber wants to make certificate modification application, it is considered as a new certificate application stated in the CPS document Section 4.1.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

Reasons for revoking subscriber and subordinate CA certificate, procedures for revocation request, revocation mechanisms and special requirements related to key compromise are defined in the CPS document Section 4.9.

Suspension procedure shall not be applied for SSL certificates.

4.10. CERTIFICATE STATUS SERVICES

Relying parties shall access revocation status records through CRL and OCSP. Operational characteristics and availability of certificate status services are defined in the CPS document Section 4.10.

4.11. END OF SUBSCRIPTION

Certificate ownership shall terminate when the certificate expires, is revoked or Kamu SM terminates certification services. In cases where Kamu SM terminates certification services or the certificate is revoked, Kamu SM shall notify the subscriber or the people specified in the agreement, if any. In case of expiration, Kamu SM shall not have to notify the subscriber; the subscriber shall be liable for following the expiration time of its certificate by its own.

4.12. KEY ESCROW AND RECOVERY

Since Kamu SM does not generate the end user keys, Kamu SM may not reissue or backup the keys of the subscribers.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

Non-technical security controls that are required to be performed while offering certificate service by Kamu SM are defined in the CPS document Section 5.

6. TECHNICAL SECURITY CONTROLS

The systems that Kamu SM generates its own key pairs with the access data and that performs all certificates management procedures are all conform to CWA 14167-1, ETSI EN 319 411-1 and CA/B Forum the BRs. Technical security controls that are required to be performed while offering certificate service by Kamu SM are defined in the CPS document Section 6.

7. CERTIFICATE, CRL AND OCSP PROFILES

The profiles of certificates and CRLs issued, and structure of OCSP service provided by Kamu SM are described in the CPS document Section 7.

7.1. CERTIFICATE PROFILE

Kamu SM creates certificates in compliance with updated versions of the documents

- ISO/IEC 9594-8/ ITU-T Recommendation X.509 v.3: “Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”,
- IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”,
- “CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates”.

Kamu SM has put restrictions on TLDs belonging to government agencies since it provides OV SSL services 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 outside these.

7.2. CRL PROFILE

Kamu SM creates CRL in compliance with the document of “IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. CRLs published by Kamu SM contain as a basis the issuer information, CRL number, issue date of CRL, date on which next CRL will be published, and serial numbers and revocation dates of revoked certificates. CRL files are signed by Kamu SM.

7.3. OCSP PROFILE

Kamu SM provides its OCSP in compliance with the document of “IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP”.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Whether or not Kamu SM meets the requirements in the CP/CPS document shall be audited at least annually. The scope of these audits is limited to OV SSL. There is no time gap between audit reports. Audits within the scope of ETSI EN 319 411-1 and CA/B Forum the BRs are made by a qualified auditor.

Information about the audit of Kamu SM compliance with its CP and CPS document is given in the CPS document Section 8.

9. OTHER BUSINESS AND LEGAL MATTERS

Information about general business and legal matters is given in the CPS document Section 9.

9.1. FEES

The subscribers are charged for the certificate issued by Kamu SM. Amount of fee and payment terms are announced in offer letter sent by Kamu SM or its corporate web page.

Kamu SM will not charge the subscribers or relying parties for the service of announcement of revocation status record via CRL or OCSP.

No fee will be charged for the procedures automatically performed over call center and electronic environment within certificate management procedures.

Kamu SM will not charge the subscribers or relying parties for access to the information and documents published in repository.

If the subscriber identifies that it fails to use its certificate as a result of audit conducted upon first delivery and it is understood that this issue arises from an error resulting from Kamu SM, fee paid for the certificate by the subscriber is refunded upon request.

9.2. FINANCIAL RESPONSIBILITY

Information about financial responsibility for relying parties and the subscribers is given in the CPS document Section 9.2.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

Kamu SM and relevant parties will not disclose their mutual commercial information. They take required measures for this purpose.

9.4. PRIVACY OF PERSONAL INFORMATION

Kamu SM maintains privacy of personal/organizational information of the certificate applicants, the subscribers or other participants within the scope of the services provided thereon.

Kamu SM does not request information except required information for issuing certificate from the certificate requesting agency. Kamu SM does not use personal/organizational information so obtained for the purposes other than offering certificate service and does not disclose the same to relying parties and does not keep available the certificate in environments accessible by relying parties without consent of the subscriber.

Kamu SM may disclose the information with relying parties with written consent of the subscriber.

Kamu SM may disclose the confidential information owned by the subscriber pursuant to judicial or administrative process.

9.5. INTELLECTUAL PROPERTY RIGHTS

Kamu SM retains intellectual property rights of all certificates and documents issued by Kamu SM and all information developed based on this CP and CPS document.

9.6. REPRESENTATIONS AND WARRANTIES

Kamu SM, subscribers and the relying parties fulfill the representations and warranties mentioned in the certificate contracts and agreements. Information about representations and warranties of CA, RA, subscribers, relying parties and other participants is given in the CPS document Section 9.6.

9.7. DISCLAIMERS OF WARRANTIES

Warranty between Kamu SM and the subscriber government agency expire as set forth in SSL Agreement.

9.8. LIMITATIONS OF LIABILITY

Limitations relating to liabilities of Kamu SM and the parties receiving certificate services are designated in SSL Agreement.

9.9. INDEMNITIES

The damages arising of failure of fulfilling the liabilities between Kamu SM and the parties of subscriber are liquidated by way of protecting rights and receivables accrued by the parties until that moment on actual basis.

9.10. TERM AND TERMINATION

The subscriber works in collaboration with Kamu SM in compliance with SSL Agreement.

The Subscribers agree that they will fulfill the requirements specified in certificate management procedures with CP and CPS document throughout the period where they receive certificate services.

Kamu SM fulfils the requirements set forth in CP and CPS document, certificate management procedures and SSL Agreement communicated to the subscriber throughout the period it has offered certificate service.

Term of SSL Agreement executed by the subscriber is as validity period of the certificate. However, if the certificate is revoked, term of the agreement also expires.

Upon expiration of SSL Subscriber Agreement, liabilities of the government agency receiving service relating to ensuring the following requirements in CP and CPS will come to an end.

Kamu SM will not be held responsible for the damages it suffers due to failure of acting in accordance with the agreement of the subscriber.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Kamu SM notifies the subscriber regarding result of certificate application in certification administration procedures and result of revocation and renewal requests.

In what circumstances and how the communication will be made with subscribers during certificate management procedures will be in detailed specified in certificate management procedures of Kamu SM.

9.12. AMENDMENTS

This document has been written by Kamu SM. Amendments likely to be made on this document may be either by way of addition or modification or Kamu SM may decide on whole renewal of the document.

Amendments made on this document will be announced by way of publicly accessing over repository of Kamu SM. Renewed document is published in repository after 1 (one) week at most and becomes effective on the date of publication.

9.13. DISPUTE RESOLUTION PROVISIONS

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

9.14. GOVERNING LAW

The laws of the Republic of Turkey shall apply for the implementation and interpretation of the CPS.

9.15. COMPLIANCE WITH APPLICABLE LAW

In the event the provisions contained in this document are found to be in contradiction with the relevant legislation to be effective thereafter, required adjustments shall be made and duly adapted.