PUBLIC

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM SSL CERTIFICATION PRACTICE STATEMENT

Version
v.3.3.3
Issue Date
04.09.2020

PUBLIC

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 Certification Practice Statement (CPS), this document has been prepared in compliance with the guidebook of "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" for the purpose of describing how Kamu SM executes its operations 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" published on https://www.cabforum.org while providing certification services. In the event of any inconsistency between the CPS document and these documents, the requirements set out in respective documents take precedence over this document.

This CPS document describes the 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

CPS document defines the roles, responsibilities, and relationships of system entities and also describes the realization 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 a 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.

CPS document has been prepared by taking "IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)" as a reference. The expression of "No Stipulation" under some subheadings refers to the document imposes no requirements related to that section. The expression of "Not Applicable" under some subheadings refers to the Kamu SM's policies forbid the practice that is the title of the section.

1.2. DOCUMENT NAME AND IDENTIFICATION

Document Name: Kamu SM SSL Certification Practice Statement

Document Version Number: 3.3.3

Date	Changes	Version
30.03.2016	Initial Release	**1.0.0**
07.03.2017	- Section 3.2.2 Authentication of Organization Identity was elaborated. - Version history was added. - Certificate profile was updated (serial number). - Section 4.9.3 SSL Certificate Revocation Form was referenced.	**1.0.1**
17.04.2017	- Section 3.2.2 Authentication of Organization Identity is updated. - Updates via annually updates of CP/CPS in April 2017	**2.1.1**
20.06.2017	- CAA records examination added.	**2.2.1**
25.09.2017	- Updates are done according to CA/B BR 1.5.0.	**3.0.0**
21.10.2017	- In domain validation, meta tag usage is replaces with file usage.	**3.1.0**
26.01.2018	- According to BR Self Assessment, minor changes are done. - Section 3.2.2 is updated with CAA Errata 5065.	**3.2.0**
07.07.2018	- ECC is added to public key algorithms.	**3.2.1**
24.10.2018	- Updates are done according to new audit standard ETSI EN 319 411-1. - Updates are done according to CA/B BR 1.6.1.	**3.3.0**
16.10.2019	- Updates within the scope of annual CPS revision.	**3.3.1**
11.06.2020	- 3.2.2.4.6 Domain validation method is changed with 3.2.2.4.18.	**3.3.2**
04.09.2020	- Issued on or after 1 September 2020, SSL certificate lifetime is reduced to 398 days.	**3.3.3**

Published on: 04.09.2020

OID: 2.16.792.1.2.1.1.5.7.1.3

This CPS 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. CPS 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. All CA services are carried out by Kamu SM personnel.

1.3.1. Certification Authorities

Kamu SM provides OV SSL certification service as a CA. For this end, there is a hierarchy consisting of a root CA, subordinate CA and OCSP certificate that are issued by root, OCSP certificate and subscriber certificates that are issued by subordinate CA. The subordinate CAs fulfill 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 this CPS.

1.3.4. Relying Parties

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

1.3.5. Other Participants

Not applicable.

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 certificate 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 the implementation of this CPS 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 : (+90) 444 5 576

Fax : (+90) (262) 648 18 00

E-Posta : bilgi@kamusm.gov.tr

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

1.5.3. Person Determining CPS Suitability for the Policy

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

1.5.4. CPS Approval Procedure

Approval of this CPS document 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 its associated Public Key.

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 online methods instantly and without interruption.

Organization Representative: A natural person who is expressed as the "Organization Contact Point" in the Application Form and the Subscriber Agreement and assigned to carry out the SSL certificate application process on behalf of the organization.

OV SSL: SSL certificate issued and maintained pursuant to "Organization Validation Certificate Policy" defined in ETSI EN 319 411-1 standard.

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.

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.

Relying parties: Natural and legal people performing a 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 has signed its own certificate.

Subordinate CA Certificate: Certificate of the subordinate CA.

Subordinate Certificate Authority: Certificate authority formed within Kamu SM, to whom is the authority to sign SSL certificates and signed by root certificate.

Subscriber: Government agency obtaining a certificate from Kamu SM.

Time stamping: Record verified by electronic signature of CA for the purpose of detecting the time when an electronic data is issued, modified, sent, received and/or saved.

Workday: Weekdays except national holidays and the weekend.

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

CAA: Certificate Authority Authorization

CEN: European Committee for Standardization

CP: Certificate Policy

CPS: Certificate Practise Statement

CRL: Certificate Revocation List

CWA: CEN Workshop Agreement

EAL: Evaluation Assurance Level

ECC: Elliptic Curve Cryptography

ETSI: European Telecommunications Standards Institute

ETSI EN: ETSI European Standard

ETSI TS: ETSI Technical Specifications

FIPS PUB: Federal Information Processing Standards Publications

IETF RFC: Internet Engineering Task Force Request for Comments

ISO/IEC: International Organisation for Standardization/International Electrotechnical Committee)

ITU: International Telecommunication Union

Kamu SM: Government Certification Authority of Turkey

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PKI: Public Key Infrastructure

RSA: Rivest - Shamir - Adleman

SAN: Subject Alternative Name

SHA: Secure Hash Algorithm

SSL: Secure Socket Layer

TLD: Top Level Domain

UTC: Coordinated Universal Time

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

A repository is the environment wherein the documents such as root and subordinate CA certificates of Kamu SM, revocation status records, CP/CPS are published uninterruptedly, securely and freely. Some critical files published in the 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 the calculation of hash values,
- OID list used by Kamu SM,
- Kamu SM CP/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. Terms and Conditions, CP and CPS documents are internationally available in the Kamu SM's website.

SSL web pages which are serviced by Kamu SM in order to test applications are given below:

Valid Certificate:	https://testssl.kamusm.gov.tr
Revoked Certificate:	https://testsslrevoked.kamusm.gov.tr
Expired Certificate:	https://testsslexpired.kamusm.gov.tr

2.3. TIME OR FREQUENCY OF PUBLICATION

The changes on CP/CPS documents are reflected agreements, forms, certificate contracts, and certification management procedures. Updated documents are promptly published.

Certificates of Kamu SM are promptly published after issuance.

Publication frequency of CRLs and frequency of updating OCSP records are specified in Sections 4.9.7 and 4.9.9.

Kamu SM CP and CPS documents are regularly updated annually. The current versions of ETSI EN 319 401, ETSI EN 319 411-1 and CA/B Baseline Requirements standards are followed and the necessary updates are made in the CP/CPS documents.

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 fulfills the following representations and warranties in regard to the repository:

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

3.1.1. Types of Names

DN (Distinguished Name) field wherein the identification information of the subscriber is revealed in the certificates issued by Kamu SM may not be left blank and name types where “ITU X.500” format is supported are used.

3.1.2. Need for Names to be Meaningful

Name values in the certificates that Kamu SM issues shall be clear and meaningful. These name values are verified by Kamu SM.

3.1.3. Anonymity or Pseudonymity of Subscribers

Anonymity or pseudonymity of the subscriber is not allowed.

3.1.4. Rules for Interpreting Various Name Forms

Name forms other than ITU X.500 are not used in certificate content.

3.1.5. Uniqueness of Names

Credentials in the content of certificates issued by Kamu SM are distinctive for each government agency. It is permitted that credentials are same in the content of certificates of the same government agency. However, credentials in the content of certificates of different agencies are prevented to be identical. Availability of only domain names, virtual server names or internal server names and IP addresses without agency information are not permitted within the certificate.

Kamu SM issues OV SSL certificates to only government agencies of Turkey. The following is included in OV SSL certificates:

- CN (Common Name) field:
  - Name of server registered on behalf of the subscriber government agency in DNS is written in “CN” field.
  - “*.<domain name>” is written in this field in OV SSL wildcard certificates. This field does not contain non-distinctive names such as “*.com” or “*.com.tr".
  - IP address or internal server name is not written in this field.
- “O (Organization)” field contains the open title or understandably abbreviated form of subscriber government agency as laid down in organizational law or other legislation.
- In cases where “OU (Organizational Unit)” field contains an organizational unit or brand name, the brand name registered in Turkish Standards Institute shall be written.
- “ST (State or Province)” field contains province information where subscriber government agency is located.
- “L (Locality)” field contains locality information where subscriber government agency is located.
- “C (Country)” field includes country code (TR) contained in ISO 3166-1 Alpha-2 standard of the country where subscriber government agency is located.
- Name of server registered on behalf of subscriber government agency in DNS contained in CN field is also written in “SAN” field. Several domain names can be written in server certificates provided that each domain name belongs to certificate applicant government agency or is under its control.

3.1.6. Recognition, Authentication, and Role of Trademarks

Certificate applicants are prohibited from using names in their certificate applications that infringe upon the intellectual and industrial property rights of others. Kamu SM does not verify whether a certificate applicant has intellectual and industrial property rights in the name appearing in a certificate application. Kamu SM reserves the right to reject certificate application or to revoke issued certificate in relation to any issue of intellectual and industrial property rights likely to occur thereon. Kamu SM does not execute any mediation activity in regard to the elimination of the said issue.

3.2. INITIAL IDENTITY VALIDATION

If applied for the first time for certificate services, the following defined methods shall be applied by Kamu SM to identify relevant agency.

Name or title of the 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.

3.2.1. Method to Prove Possession of Private Key

Certificate signing request issued by the applicant during SSL certificate application shall be signed by a private key. In this way, ownership of private key shall be verified.

3.2.2. Authentication of Organization and Domain Identity

Authentication of government agencies having requested OV SSL certificate from Kamu SM shall be performed by way of verification from official correspondences made between Kamu SM, relevant government agency and relevant channels of domain ownership (nic.tr).

3.2.2.1. Identity

Identity and address verification steps:

- The identity and head office address of the government agency requesting certificate is checked whether it is same as the information in the certificate signing request based on the legal documents.
- Organization representative executing application procedures is verified by the legal documents that it has right to apply on behalf of the agency. Through the phone numbers verified according to this, it is requested to confirm the application by calling the organization representative.
- Continuity of operation should be verified with a current official document to be submitted by organization representative or the people authorized to issue an official document on behalf of government agencies.
- 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.

3.2.2.2. DBA/Tradename

Kamu SM does not allow that Subject Identity Information including DBA or tradename.

3.2.2.3. Verification of Country

Kamu SM only issues certificates to Turkish Government Agencies.

3.2.2.4. Validation of Domain Authorization or Control

Domain ownership verification steps:

- It is first checked that the domain name is a government agency domain name with the TLDs listed in Section 7.1.5.
- Full domain name indicated in application form is verified through “nic.tr”. “nic.tr” is the government entity that keeps “.tr” top-level domain in Turkey. It is checked whether the domain name stated ownership in the application form is same as the information provided by nic.tr. It is also checked whether the domain name specified in the application form is the same as the domain name in the certificate signing request.
- Kamu SM requests change on a page submitted in the domain name to test the agency’s control over the domain name. The requested change is the publication of the request token which will be generated from the information used in certificate signing request by the government agency, in the file which is served at .well-known/pki-validation/ directory and named as “kamusmdv.txt” on the domain. The request token which is requested to publish by Kamu SM is indicated as the SHA-256 hash value of the certificate signing request used by the government agency to certify the domain name. After the request token value is published, Kamu SM makes the necessary checks and verifies the domain name ownership.

The method defined in BR version 1.7.0 Section 3.2.2.4.18 is used for domain ownership validation and control. The effective version of BR and the method used during the domain ownership and control validation process are recorded.

3.2.2.5. Authentication for an IP Address

Kamu SM does not issue SSL certificates to directly IP addresses.

3.2.2.6. Wildcard Domain Validation

In wildcard certificate validation, It is first checked that FQDN does not contain "*" on the left side of high-level top domain such as "*.com" or "*.com.tr". To verify domain name ownership for wildcard certificates, all the above items are applied. Additionally, for the website having "*.<domain name>", It is requested to publish request token identified by Kamu SM.

3.2.2.7. Data Source Accuracy

All applications made to Kamu SM shall be supported with legal documents that shall authenticate the following information and some of this information shall be included within the Subject field:

- Legal title of agency – Name of the government agency to be included in O field in the certificate (PUBLIC)
- Organization unit name – Unit name of the agency to be included in OU field in the certificate (PUBLIC)
- Address of agency (Province/District/Zip Code) (PUBLIC)
- Tax number
- Organization representative information
- Full domain name (FQDN - Fully Qualified Domain Name) (PUBLIC)
- Full name, e-mail address and contact information of administrator owning a domain name
- PKCS#10 Certificate Signing Request
- Commitment letter

All information above need to be provided in the application process. After application form is received, Kamu SM carries out authentication in mainly two parts. Firstly, the identity and address of the government agency are verified. Secondly, the domain ownership of applicant government agency is verified. Both verification procedure conforms to CA/B Forum the BRs document.

3.2.2.8. CAA Records

As part of the issuance process, after all other validation has been completed, Kamu SM checks CAA records for all domains listed in the certificate according to the procedure in RFC 6844 Errata 5065 (DNS Certification Authority Authorization (CAA) Resource Record). "kamusm.gov.tr" domain name is recognized in a CAA record's issue and issue wild property tags. If there exists no problem in CAA record, the certificate is issued within the TTL of CAA record. In the case of lookup failure, the certificate can be issued if the failure is outside Kamu SM's infrastructure or the lookup has been re-tried at least once. Each CAA record is logged whether the certificate is issued or not issued.

3.2.3. Authentication of Individual Identity

Organizational application rather than the individual application is accepted since Kamu SM offers OV SSL service to government agencies.

3.2.4. Non-Verified Subscriber Information

SSL certificates issued by Kamu SM do not contain any non-verified information.

3.2.5. Validation of Authority

It shall be performed as described in Section 3.2.2.

3.2.6. Criteria for Interoperation or Certification

No stipulation.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-Key

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 Section 3.2.

3.3.2. Identification and Authentication for Re-Key After Revocation

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 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.

To ensure time consistency during certificate revocation, Kamu SM synchronizes all servers with UTC at least once every 24 hours.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This part describes the procedures performed in certification management processes. Kamu SM is independent of other organizations in the establishment and maintenance of services in accordance with the certificate policies related to the issuance and revocation of certificates. Kamu SM is also certified organization that provides the impartiality of the processes related to the issuance and revocation. Kamu SM personnel responsible for certificate issuance and revocation management are prohibited by law to conduct commercial and financial transactions that would damage the security of the CA services. Details relating to the processes are revealed on website of Kamu SM.

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Government agencies can apply to Kamu SM for SSL certificate. These applications shall be made corporately by an organization employee duly authorized. The agency shall complete SSL Agreement setting forth requirements of certificate services to be obtained from Kamu SM and Secure Server Certificate Request Form and shall send them to Kamu SM with signature and seal/stamp. Organization

employee may not individually make an application without the request of the government agency. All previously revoked certificates and previously rejected certificate requests are logged.

4.1.2. Enrollment Process and Responsibilities

Responsibilities of the government agency having applied for SSL certificate is as follows:

- It shall send Secure Server Certificate Request Form as incorporating all information with requirements set out in this CPS document and SSL Agreement to Kamu SM with signature and seal/stamp. The agency shall be liable for following up the information sent to Kamu SM and notifying Kamu SM in case of modification in this information.
- The agency shall generate key pair by itself and shall create Certificate Signing Request (CSR) as to prove that private key belongs to itself and sends this to Kamu SM from corporate e-mail address.
- The agency shall take all required measures for protecting the confidentiality and integrity of its private key.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

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.

The documents provided for the application process cannot be re-used. Kamu SM can use additional methods for authentication of high-risk certificate requests.

No Delegated Third Party is authorized by Kamu SM in performing identification and authentication functions.

Kamu SM checks CAA records for all domains listed in the certificate according to the procedure in RFC 6844 Errata 5065. Policy on processing CAA DNS Records is given in Section 3.2.2.8.

4.2.2. Approval or Rejection of Certificate Applications

In case of required forms and documents are fully completed in accordance with application procedures of Kamu SM and the principles described in Section 3.2, certificate application shall be accepted. Those whose application has been accepted are defined in the system of Kamu SM and certificate issuance process shall be initiated.

Kamu SM shall reject certificate application in case any of the circumstances occurs:

- Required forms and documents are not duly completed in accordance with application procedures of Kamu SM and the principles described in Section 3.2,
- The applicant fails to satisfactorily respond the queries relating to verification of the information and documents in a timely manner,
- The organization has no official record,
- The emergence of strong conviction presuming that issuance of SSL certificate may damage the reputation of Kamu SM,
- Presence of falsification, error, missing approval, missing information or inaccurate information in the documents declared during certificate application,

- CSR file sent to Kamu SM not meeting technical criteria.

Information relating to those whose application has not been accepted shall be notified via e-mail or by calling. E-mail and phone information of the applicant is the information declared during application. After required adjustments are made and missing parts are completed, the applicant may re-apply.

4.2.3. Time to Process Certificate Applications

In so far as the application is accurate and complete in accordance with the principles contained in Section 3.2 and the procedures of Kamu SM, the application shall be taken into consideration within at the latest 3 (three) working days following delivery of relevant documents to Kamu SM.

After considered certificate application is accepted pursuant to the principles contained in Section 4.2.2, its issuance shall be performed within at the latest 2 (two) working days.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

Certificate applications accepted in pursuance of the principles contained in 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.

Certificates issued by root can only be generated by the CA certificate issuance personnel and system operator's order.

4.3.2. Notification of Certificate Issuance

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

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscriber shall check whether or not the information contained in the 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.

SSL certificate shall be deemed to have been accepted in case of no return within 10 working days following sending it to the applicant.

4.4.2. Publication of the Certificate by the CA

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

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscriber shall use its certificate and private key within the framework of the terms and conditions contained in the agreement of relevant subscriber and in CP/CPS document with other regulations and standards being subjected to.

Subscriber shall be liable for protecting its private key against unauthorized access. Private key corresponding to SSL certificate may only be used within the purposes specified in the “Key Usage” field of the certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Public key contained within the certificate of the subscriber may be used for verification purposes by relying parties. Relying parties shall be liable for checking the validity of CA certificate issuing the certificate and the certificate itself, for verifying that the certificate is used in line with the purposes specified in the “Key Usage” field and for conforming to use terms specified in CP/CPS.

If the certificate validation is unsuccessful, the procedure should not be performed based on the certificate.

Kamu SM shall not be responsible for a failure of relying parties to fulfill the said requirements thereon in use of public key and certificate.

4.6. CERTIFICATE RENEWAL

Certificate renewal refers to the 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 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 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 a certificate modification application, it is considered as a new certificate application stated in Section 4.1.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

The subscriber shall apply to Kamu SM for revocation of its certificate in the following cases:

- Suspecting confidentiality of its private key,
- Modification in the information contained in the certificate,
- Termination of domain name ownership.

Kamu SM shall revoke the subscriber certificate within 24 hours in the following cases:

- The subscriber requests in writing that the Kamu SM revoke the certificate,
- Kamu SM obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise,

- Kamu SM obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name the certificate should not be relied upon.

Kamu SM shall revoke the subscriber certificate within 5 (five) days in the following cases:

- Determining the certificate was not issued in accordance with CA/B Baseline Requirements or CP/CPS,
- The emergence of forgery or inaccuracy of the information of the subscriber in the certificate,
- The emergence of modification in the information contained in the certificate,
- Determining use of the certificate in contradiction with the requirements set forth in SSL Agreement and CP/CPS document,
- Issuing a notification to Kamu SM indicating that a court or an authority has revoked domain name ownership or use the authority of the subscriber, or this case is identified by Kamu SM,
- Key size or cryptographic algorithms used in the issuance of SSL certificate becoming deprecated,
- Termination of operation of Kamu SM and failure of continuation of management of issued certificates by other CAs,
- Kamu SM is informed by the organization or it is determined that the Subscriber is not legally authorized to submit the SSL Application.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

Kamu SM shall revoke the subordinate certificate within 7 (seven) days in the following cases:

- Determining use of the certificate in contradiction with the requirements set forth in CA/B Baseline Requirements, CP/CPS documents, and Terms and Conditions,
- Compromise of the private key used by Kamu SM for signing the certificate,
- Key size or cryptographic algorithms used in the issuance of SSL certificate becoming deprecated,
- The emergence of inaccuracy of the information in the certificate,
- Termination of operation of Kamu SM and failure of continuation of management of issued certificates by other CAs.

4.9.2. Who Can Request Revocation

The organization representative is entitled to request the revocation of the certificate issued by Kamu SM. In cases of the circumstances provided in Section 4.9.1.1, Kamu SM is also entitled to revoke the certificate. However, in case Kamu SM revokes the certificate, Kamu SM informs the agency and provides the reason(s) for revocation.

4.9.3. Procedure for Revocation Request

SSL certificate revocation application shall be made by the organization representative with the “SSL Certificate Revocation Form”. Applicants can find the form in Kamu SM web page. It should be filled in completely and sent to Kamu SM with signature and seal/stamp. In case of an urgent revocation, the organization representative should send the scanned form from his corporate e-mail address to ssliptal@kamusm.gov.tr e-mail address designated for revocation requests published in the Kamu SM

web page and also he calls Kamu SM for revocation. In this case, after the required authentication procedures, Kamu SM shall revoke the certificate.

Kamu SM notifies the agency about the revocation of its certificate via e-mail and the revocation is reflected CRL and OCSP as described in Section 4.9.5.

In case of revocation of root or subordinate CA certificates of Kamu SM, revocation status shall be announced to relevant parties as soon as possible. All certificates bearing the signature of root or subordinate CA shall be revoked and their owners shall be duly notified via e-mail or SMS.

4.9.4. Revocation Request Grace Period

Revocation request grace period refers to the maximum time that the subscriber may delay the certificate revocation request. The subscriber should communicate its revocation request to Kamu SM within the shortest time possible. Kamu SM shall not be held responsible for the issues of the subscriber arising from the delay of revocation request.

4.9.5. Time within which CA Must Process the Revocation Request

Kamu SM verifies the revocation applications at most 24 hours after receiving the request. If the revocation request is valid, the certificate is revoked within 1 hour. This revocation information will be reflected to the OCSP server immediately and to the CRL file at most 1 hour. Revoked certificates cannot be reinstated.

If there is an error spotted in the SSL certificate by the third party, an investigation request may be submitted to Kamu SM. In the next 24 hours, Kamu SM does investigate the SSL certificate and provide a preliminary information on its findings to both the subscriber and the third party who request the investigation. Kamu SM decides the revocation status of the certificate in accordance with the Section 4.9.1.1 and informs the subscriber and the related party about the certificate status.

4.9.6. Revocation Checking Requirement for Relying Parties

Revocation status records shall not require authentication and are freely and publicly accessible for everyone. Kamu SM shall maintain continuity of access for revocation status records.

Relying parties shall be liable for checking the validity of certificates using one of CRL or OCSP methods prior to performing any procedure based on the certificates.

Relying parties shall check that CRL file that relying parties have performed certificate validity check or revocation status record obtained from OCSP service has been signed with the Kamu SM private key. Validity checks required to be performed by relying parties are described in Section 9.6.4.

4.9.7. CRL Issuance Frequency

CRL wherein the certificate revocation information of end users is available shall be published minimum once a day. The validity period of this CRL is maximum 36 hours. The new CRL is published before the time specified in the nextUpdate field in CRL. CRL file survives until its expiry time although newer one is published.

CRL files containing subordinate CAs revocation information shall be published minimum once a year. The published CRL has a validity period of at most 1 (one) year. If a subordinate CA certificate is revoked, a new CRL shall be published immediately. CRL files published by Kamu SM shall be archived.

4.9.8. Maximum Latency for CRLs

CRL shall be published within at the latest 10 minutes as of the moment of its issuance.

4.9.9. On-Line Revocation/Status Checking Availability

Kamu SM shall uninterruptedly publish revocation status records of SSL certificates over OCSP. Applications with OCSP support shall receive revocation status of SSL certificates over http://ocspssls1.kamusm.gov.tr and revocation status of Kamu SM subordinate CA certificates over http://ocspsslkoks1.kamusm.gov.tr.

4.9.10. Online Revocation Checking Requirements

Relying parties shall be obligated to check the revocation status of a certificate in line with the principles set out in Section 4.9.6 prior to relying on this certificate. If technical facilities are eligible, performing certificate revocation check over OCSP is the method recommended by Kamu SM.

Kamu SM OCSP servers support requests and responses over HTTP in accordance with RFC 6960 [X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)]. Kamu SM OCSP servers can respond to GET and POST requests made by subscribers. When a revocation query is issued for a certificate serial number that does not exist in the Kamu SM system, the OCSP server returns an "UNKNOWN" as a response. The validity interval of an OCSP response is 8 hours.

4.9.11. Other Forms of Revocation Advertisements Available

Kamu SM shall not provide revocation status advertisement methods rather than CRL and OCSP.

4.9.12. Special Requirements Related to Key Compromise

If confidentiality or security of any CA private key of Kamu SM is under suspicion, the certificate related to this private key and all the certificates under this CA certificate shall be revoked, and certificate owners shall be duly notified via e-mail.

In cases where Kamu SM discovers or has reasons to believe compromise of subscriber's key, it shall revoke the certificate and notify the subscriber. New certificate issuance procedures shall be initiated within the shortest time possible in all certificate revocation procedures originating from Kamu SM.

4.9.13. Circumstances for Suspension

Suspension procedure shall not be applied for SSL certificates.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

Relying parties shall access revocation status records through CRL and OCSP.

4.10.1. Operational Characteristics

Relying parties may access revocation status records from CRL files that Kamu SM publishes. Access information to CRL files is provided in Section 2. Whenever relying parties want to check the revocation status of certificates, they shall copy CRL file from Kamu SM repository and shall fetch the status information. Revoked certificates will not be removed from the CRL and OCSP before their expiration dates.

Relying parties with OCSP client support may access revocation status records from OCSP service. Access address of OCSP service is provided in Section 4.9.9. Whenever relying parties want to check validity status of certificates, they shall query the status of certificates over OCSP service.

Relying parties may access revocation status information via CRL and OCSP until the certificate expires.

4.10.2. Service Availability

Kamu SM shall take all required measures for providing CRL and OCSP services uninterruptedly on a 24/7 basis. Kamu SM maintains OCSP service to provide a response time of less than 10 seconds.

4.10.3. Optional Features

No stipulation.

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

This section outlines non-technical security controls that are required to be performed while offering certificate service by Kamu SM.

Kamu SM carries out a risk assessment to evaluate the risks related to certification management services. Kamu SM identifies appropriate risk treatment measures and controls, taking account of the risk assessment results. Kamu SM provides the necessary resources to implement the risk treatment measures and controls chosen. All risks identified, including residual risks, are approved by the Kamu SM management. All risks are reviewed at least once a year.

Kamu SM Information Security Policy has been approved by management. It is available on the Kamu SM website for relevant external parties. The relevant parties are informed about the changes made in the Information Security Policy.

System configurations are reviewed every 3 (three) months to detect information security policy violations via sampling.

Kamu SM identifies and maintains an inventory of all information assets. Kamu SM handles access authorization and security of assets in accordance with requirements of the information classification scheme.

5.1. PHYSICAL SECURITY CONTROLS

Kamu SM operates its systems in physically secured locations that are equipped with security precautions such as access control systems against unauthorized access. They are protected from external as well as internal malicious activities. A record of all access to secure areas is maintained.

Private keys of the Kamu SM's root certification authority are physically separated from the area where normal operations take place. The area can be accessed by at least two authorized personnel.

5.1.1. Site Location and Construction

Kamu SM operations are conducted within facilities in Gebze and Ankara. Gebze facility is located away from the city where the disasters such as fire, flood, earthquake, lightning and air pollution have minimal impact. Access to areas and the buildings are protected by multiple tiers of physical security, video monitoring and authentication including hi-sec interlocking doors that only allows single person entry or exit. Ankara facility is a metropolitan area with levels of physical access controls.

The building is suitable for the high-security operations designed to deter, prevent and detect covert/overt penetration. The building is constructed of resistant materials.

Power supplies, communication units, ventilation, and fire suppression systems ensure reliable operation. Proper safety precautions are taken against earthquakes, flood, and other disasters. Software and hardware modules, and the archives are restricted in accordance with segregation of duties requirements to prevent unauthorized modification, substitution or destruction. Unauthorized personnel and unescorted visitors are not allowed into such sensitive areas.

5.1.2. Physical Access

Access to hardware systems and archives of Kamu SM are under control. Access to the building is provided by advanced access control devices under the control of security guards.

Access to the rooms where software and hardware tools belonging to Kamu SM system are present, electronic or paper information is maintained, and where the system is operated and managed, are made with advanced access control devices that perform biometric controls. A single person cannot access to secure areas, a non-authorized person shall be accompanied by at least an authorized person to work inside the secure area. Unauthorized personnel cannot enter rooms where the system is installed. The unauthorized access to the rooms where the system is installed is regulated in accordance with special access instructions for hardware maintenance or such an unusual purpose.

5.1.3. Power and Air Conditioning

The following power units are utilized to support the operations of Kamu SM and provide its continuity:

- Transformation units
- Distribution panels
- Transformer
- UPS devices

- Dry accumulator
- Emergency power generator

The building is equipped with uninterrupted heating/air ventilation systems that are used to prevent overheating and to maintain a suitable humidity level.

5.1.4. Water Exposures

The necessary precautions are taken to minimize the damages arising from the floods and water exposures at Kamu SM facilities.

5.1.5. Fire Prevention and Protection

Kamu SM facilities are equipped with smoke detection systems. Necessary precautions are taken to ensure secure facilities are protected from exposure to flame and smoke.

5.1.6. Media Storage

All media containing production software, production data, system audit, and archive are protected physically and electronically against corruption, aging and accidental damage. Media are backed up on-site and off-site.

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are destroyed irreversibly. Cryptographic devices, smart cards, and other devices containing private keys or keying materials are physically destroyed and zeroized according to industry best practice. Another waste is disposed of in accordance with normal waste disposal requirements.

5.1.8. Off-Site Backup

Kamu SM has a geographically separate, remote disaster recovery center for backup in different locations. Kamu SM stores the components deem necessary in safe spaces in a different physical location to ensure the continuity of the system. The locations, where the backups are located, comply with all the security and functional requirements of the main system. Access to backup servers/media is restricted to authorized personnel only.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Roles of personnel employed in Kamu SM have been identified in accordance with CWA 14167-1 and ETSI EN 319 401 standards and have been classified as follows:

Kamu SM Administrator: Kamu SM Administrator is responsible for managing all administrative and technical activities for fulfilling strategic objectives of Kamu SM.

Security Personnel: Security Personnel is responsible for implementing security policies.

System Administrators: System Administrators are responsible for managing information technology infrastructure for sustainability of certificate service.

System Operators: System Operators are responsible for operation, backup and recovery activities for all system components.

System Auditor: System Auditor is responsible for reviewing and inspecting archive and audit logs relating to certificate service.

Certificate Enrolment Personnel: Certificate Enrolment Personnel is responsible for receiving certificate applications/revocation requests, verifying the application documents and authenticating identity of the organization.

Certificate Issuance Personnel: Certificate Issuance Personnel is responsible for the verification of domain authorization and the CSR file and also issuance of the certificate.

5.2.2. Number of Individuals Required per Task

Kamu SM requires at least presence of 2 (two) personnel at the same time for issuing certificates of CA and end users, revocation of CA certificate, and backing up CA private keys within another cryptographic module.

5.2.3. Identification and Authentication for Trusted Roles

Verification of identity and authentication of the personnel are performed in each step of Kamu SM procedures. In this way, only access of authorized personnel is established for each system unit. Access to some of the units in the system is permitted by different levels of authorizations. In order for accessing these units, the authentication is made and the operations can be performed in accordance with the authorization levels.

Verification of identity within Kamu SM system is performed with up to date cryptographic methods by using secure hardware tools, passwords, secret questions, and biometric data.

User account authorization and management are based on the Kamu SM Access Management Policy.

5.2.4. Roles Requiring Separation of Duties

Separation of duties among trusted roles meets CWA 14167-1 standard at least.

Separation of duties exist among;

- Certificate Issuance Personnel and Certificate Enrolment Supervisor,
- System Auditor and other roles,
- System Administrator and Security Personnel and System Auditor.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

Personnel is selected from those with requisite background, qualifications, and experience that shall meet the operational and security requirements of the system. Personnel to be employed by Kamu SM are comprised of qualified people with knowledge and experience in relevant fields such as system security, database management, electronic signature technologies and applications, and certificate management.

5.3.2. Background Check Procedures

All trusted personnel have to undergo background checks before access is granted to systems. Prior to commencement of employment, it is investigated whether or not the personnel has been convicted for any reason. Judicial records of the person are examined. A person can be started to work after successful security investigation. An employee is not authorized to access systems without taking Information Security Awareness Training.

5.3.3. Training Requirements and Procedures

Personnel is required training prior to the active commencement of their employment in Kamu SM. Security policies, technical and administrative system operations, processes related to employment, duties, and responsibilities are described in the training for newly recruited personnel.

Kamu SM provides training to its employees at least once a year to raise awareness about information security policies, cybersecurity, and social engineering attacks.

5.3.4. Retraining Frequency and Requirements

Kamu SM provides refresher training and informational updates to ensure that personnel maintains the required level of proficiency to perform their job responsibilities competently and satisfactorily. Basic initial training is provided for newly recruited personnel.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

According to the information security policy breach and the extent of the violation, legal action and disciplinary process are initiated in the event that Kamu SM employee create wholly or partly forged electronic certificate, impersonate or falsify the electronic certificates that are currently established, create electronic certificate without authorization or using these electronic certificates, and in the other unauthorized actions.

5.3.7. Independent Contractor Controls

Kamu SM does not employ Delegated Third Parties.

5.3.8. Documentation Supplied to Personnel

Personnel is provided with required guidelines and supporting documents in relation to their job responsibilities. These include technical and operational documents required for CPS and Kamu SM to execute CA operations.

5.4. AUDIT LOGGING PROCEDURES

Logs of the events related to key and certificate management and system security performed during operation of Kamu SM are duly stored. Kamu SM maintains electronic or manual logs of the following events for core functions. These logs are examined by the officials when deemed necessary during audits. The clock of the server where electronic records are kept is synchronized with UTC at least once a day.

5.4.1. Types of Events Recorded

Logs of the events performed electronically or manually related to the events performed below are stored:

- Kamu SM key lifecycle management events
  - Key generation
  - Key backup
  - Key destruction
  - Cryptographic device lifecycle management events

- Certificate issuance and revocation applications
  - Kind of identification documents presented by the Certificate Applicant
  - Record of unique identification documents taken during application
  - Forms or documents taken electronically or manually during application
  - The storage location of copies of applications and identification documents
  - All application information received validly and invalidly
- Certificate lifecycle management events
  - Certificate issuance
  - Certificate revocation
  - Issuing CRL
- Other events related to security
  - All successful and unsuccessful access attempts to system
  - Security system actions performed by personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures, and other anomalies
  - Security device/software events (Firewalls, IPS, HIDS, Router etc.)
  - Kamu SM facility visitor entry/exit

Log content, log time and the name of personnel causing the creation of log are found in logs.

5.4.2. Frequency of Processing and Archiving Audit Logs

System operation logs are reviewed periodically. Reviews are conducted on weekly basis for possible security issues. Logs are examined periodically for security and operational events. In addition to this, logs stored in the system are reviewed in case of alarms or monitoring irregularities. Actions taken based on reviews are also documented.

Electronic or manual logs of the information received from subscribers during certificate application may be examined by virtue of legal actions or once deemed necessary within the certificate lifecycle period.

5.4.3. Retention Period for Audit Log

Audit logs are stored within the system at least for 2 (two) months after reviews and thereafter archived. Audit logs are made available to qualified auditor upon request.

5.4.4. Protection of Audit Log

The following precautions have been taken for keeping audit logs of Kamu SM under security either electronically or manually:

- Unauthorized people may not access the systems where electronic audit logs are stored.
- Manual audit logs are stored in locked rooms and can be accessed only by the authorized personnel.

- The records shall not be deleted, altered or destroyed within the required legal period. In this direction, necessary security measures are taken.
- Audit logs posing criticality in terms of system operation are signed digitally and stored. In this way, all kinds of modifications likely to occur in critical records will be noticed by the system.
- Critical information is stored encrypted with keys of Kamu SM, when necessary.

5.4.5. Audit Log Backup Procedures

Considering criticality of the system, online backups of necessary logs are taken regularly on a daily basis when the system is not intensively used. Tape library for meeting backup requirement and backup management software for automated backups are available. Critical audit logs are backed up in secure disaster recovery facilities located in geographically remote cities.

5.4.6. Audit Log Accumulation System (Internal vs. External)

Audit logs are automatically collected on the levels of application, network and operating system. Automatic audit log collection operates from start-up to shut-down of the system.

5.4.7. Notification to Event-Causing Subject

Kamu SM system user, prompting the event and causing audit log creation, is notified by the system regarding audit log creation.

5.4.8. Vulnerability Assessments

Technical security controls mentioned in Section 6.5, 6.6 and 6.7 are implemented for the systems where audit logs are stored.

Kamu SM periodically conducts weakness assessment and records these assessments. Weaknesses recorded are processed based on risk assessment events.

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

In addition to the logs specified in Section 5.4.1, the 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
- 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
- NTP synchronization logs of systems that used for certification processes

5.5.2. Retention Period for Archive

Archived data and documents are retained for a period of minimum 7 (seven) years.

5.5.3. Protection of Archive

Archived data and documents are electronically and physically protected safely to prevent unauthorized monitoring, modification, and deletion. Only authorized personnel have access to archives. Media, where archives are retained, is selected in a way that will prevent damaging of archives during time frame set out in 5.5.2.

5.5.4. Archive Backup Procedures

Electronic archives containing critical information are backed up in pursuance of Kamu SM business continuity policy.

5.5.5. Requirements for Time-Stamping of Records

Kamu SM adds time stamping to records where it deems necessary.

5.5.6. Archive Collection System (Internal or External)

Archives are collected according to relevant procedures either electrically or manually.

5.5.7. Procedures to Obtain and Verify Archive Information

Archive information is obtained from authorized personnel. In case of more than one archive pertaining to the same information, archives are compared and their accuracy is checked.

5.6. KEY CHANGEOVER

Keys and certificates of Kamu SM may be renewed as they expire or because of security concerns. Prior to the expiration of the certificate of Kamu SM, key changeover procedures are done. Key changeover process requires the following:

- Actions are initiated at the latest 3 (three) years before the expiration of the root certificate lifetime; 1 (one) year before the expiration of the subordinate certificate. Issuing certificate with the old key is ceased.
- Old Kamu SM certificate continues to be published in order for certificates to be verified which are signed with old Kamu SM private key.
- If CRL file and certificates are signed with the same private key, Kamu SM continues to sign CRLs with the same private key until the last expiration date of the certificates issued using this private key. CRL file created for newly issued certificates is signed with new Kamu SM private key.
- Kamu SM announces the information of renewal of its keys on http://www.kamusm.gov.tr web address and notifies the government agencies to which it provides certificate service.

5.7. COMPROMISE AND DISASTER RECOVERY

Information systems monitored for possible security violations and detected violations are reported. Any addressed critical vulnerability handled within a period of 48 hours after its discovery. Start-up and shutdown of the logging functions, availability, and utilization of needed services are monitored.

5.7.1. Incident and Compromise Handling Procedures

In case of a compromise, (incident or security vulnerability etc.) designated processes are operated so as to securely restore certificate management system within the shortest time possible, to notify affected parties of the incident within 24 hours and to mitigate the damages.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data are Corrupted

If Kamu SM determines that its computing resources, software, or data operations have been compromised, Kamu SM will investigate the extent of the compromise and the risk presented to affected parties.

Compromise of computing resources, software, or data operation is reported and required event management process is initiated for remedying failure/error.

Active devices, servers and storage network components to be used in redundant structure to ensure business continuity and disaster recovery center is established for critical processes. The storage unit is able to synchronize data with the data storage unit located at a different point. The process of remedying the failure contains an investigation of the cause of failure, remedying the error and migrating Kamu SM services to trusted redundant media when deemed necessary.

5.7.3. Recovery Procedures After Key Compromise

Upon the suspected or known compromise of the private key of Kamu SM used in signing the certificate, the relevant certificate is revoked within the shortest time possible and following operations are performed within the business continuity plans:

- Certificate's revoked status of Kamu SM is published together with the grounds for revocation within the shortest time possible over http://www.kamusm.gov.tr website and notifies all affected parties in writing.
- Kamu SM makes a statement indicating to what extent the subscribers will be affected and issues a notice to affected parties not to rely on the certificates signed with old private keys.
- Kamu SM states revoked status of its certificate in CRL file.
- Some or all of the certificates issued by Kamu SM are revoked. Subscribers are notified of certificate's revoked status within the shortest time possible.
- Kamu SM ceases to respond to certificate requests.
- Affected parties are notified in the ongoing basis in relation to the status of Kamu SM.
- Kamu SM processes destruction of the private key.
- Kamu SM delivers a new certificate to the parties by generating a new key pair and issuing a certificate.
- Upon renewal of key pair of Kamu SM, the process of issuing new certificates instead of revoked ones is initiated in line with the requests received from the users.

5.7.4. Business Continuity Capabilities after a Disaster

Kamu SM defines required procedures and processes for restoring the system at the earliest and secure resumption of the system following a compromise or disaster in Kamu SM Business Continuity Plans.

Kamu SM maintains a disaster recovery facility located at a separate city. Kamu SM backups copies of essential information and software in accordance with backup management policy which identify essential information, time period and personnel roles and when necessary recovery procedure is applied. For maintaining business continuity, backups of data stored in Kamu SM head office are also retained in disaster recovery facility.

Kamu SM periodically revises and tests Kamu SM Business Continuity Plans enabling restoration and recovery after a compromise. Kamu SM takes necessary measures to prevent the repetition of failures.

5.8. CA OR RA TERMINATION

In the event that it is necessary for Kamu SM to cease operations for any reason whatsoever, it will perform the following operations within Kamu SM certification services termination plan:

- In case of termination of CA operations for any reason, Kamu SM notices it's upper authority and all government agencies to whom it provides certificate services at least 3 (three) months before termination.
- Kamu SM makes a public announcement that it will cease to act as CA according to the legislation.
- Kamu SM does not accept any certificate application from its announcement to cease to act as CA and does not issue a new certificate.
- Kamu SM revokes the certificates it has issued and announces their revocation status information to relying parties via CRL and OCSP. Subscribers are notified of the revocation of certificates.
- Kamu SM continues to publish the last CRL file until the expiration of all revoked certificates.
- Kamu SM continues to publish its certificate corresponding to the private key used for signing CRL throughout the validity period of the CRL file.
- Kamu SM destroys private key used for signing certificates.
- Kamu SM maintains all relevant logs and archives minimum for a period of 7 (seven) years.

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 all conform to CWA 14167-1, ETSI EN 319 411-1 and CA/B Forum the BRs.

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

Key pairs of root and subordinate CAs shall be generated by using secure software and/or hardware meeting FIPS-140 or EAL4+ standards, passed from the testing required for secure key generation, in closed network environment under the supervision of several trained personnel in a secure room where unauthorized personnel cannot access. Generated private keys shall be stored within the secure cryptographic module. The module cannot be moved out of the secure room. All procedures conducted shall be recorded and shall be approved by the personnel having performed the procedure.

The requirements of the documents of ETSI EN 319 411-1 and the BRs shall be met during generation of key pairs.

Cryptographic module where the private key is stored conforms to the standards laid down in Section 6.2.1.

Key pair generation for SSL certificates shall be performed by the requesting party. Kamu SM shall not issue PKCS#12 file for the end users.

6.1.2. Private Key Delivery to Subscriber

Since key pair generation for SSL certificates is performed by the party requesting the certificate, delivering private key to its owner is out of the question.

6.1.3. Public Key Delivery to Certificate Issuer

Following acceptance of the application, SSL certificate applicant shall deliver its public key in PKCS#10 format to Kamu SM via e-mail by using its corporate e-mail.

6.1.4. CA Public Key Delivery to Relying Parties

Root and subordinate CA certificates shall be made available for access of the relying parties through the Kamu SM repository.

6.1.5. Key Sizes

RSA key sizes of root and subordinate CA are 2048 bits. RSA key size of OCSP certificate is 2048 bits.

For SSL certificate RSA key pairs Kamu SM ensures that:

- The modulus size, when encoded, is at least 2048 bits, and;
- The modulus size, in bits, is evenly divisible by 8.

For SSL certificate ECDSA key pairs Kamu SM ensures that the key represents a valid point on the NIST P-256 or NIST P-384 elliptic curve.

6.1.6. Public Key Parameters Generation and Quality Checking

Kamu SM uses the RSA with SHA-256 algorithm for key generation of the root, subordinate and OCSP certificates and performs key generation according to the features specified for the RSA algorithm in the CA/B Forum the BRs Section 6.1.6.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

For what purposes the keys issued by Kamu SM shall be used shall be specified in the “Key Usage” and “Extended Key Usage” extensions in the certificates.

Private key corresponding to Kamu SM root certificate is used for signing subordinate CA certificates and CRLs. Certificate chain used in signing subscriber certificates is detailed in Appendix-A. OCSP certificates delegated by root and sub-root are used for signing OCSP responses.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

Kamu SM private keys shall be generated by using secure hardware and/or software and shall be stored in the secure cryptographic module and shall not move outside of this module.

The cryptographic module has the following security functions specified:

- It provides confidentiality and integrity throughout the validity period of the private key.
- It meets identification and authentication functions in accessing the module.
- It can be defined in a manner that access authority shall be under the control of several authorized personnel.
- It restricts access to the services offered in line with the roles defined for the user.
- All kinds of physical measures likely to lead to tampering with use and unauthorized access to the module have been properly taken.
- In case of attempting unauthorized access, the module shall delete the data inside it.
- It enables secure backup of the private key.
- The cryptographic module shall meet a minimum one of the following security standards: FIPS 140-1, 140-2, 140-3 or higher.
- Cryptographic modules that have retired and/or malfunctioned cannot be taken out of the secure area and destroyed in accordance with the destruction procedure.

6.2.2. Private Key Multi-Person Control

Access to the room where Kamu SM private keys exist shall be established by being complied with the principle of separation of duties and under the presence of minimum 2 (two) different personnel. Access attempts made by people other than authorized personnel shall be blocked via required controls.

6.2.3. Private Key Escrow

Not applicable.

6.2.4. Private Key Backup

Backup procedure of Kamu SM private keys shall be performed by several authorized personnel together. The backup procedure shall be performed under equivalent security measures as security established for operative private keys. Backed up private key shall be kept within a physically and electronically secure cryptographic hardware, as blocked for access of unauthorized people. This secure hardware device shall be kept in an environment having the same security requirements with the environment where the operative private keys exist.

Private keys of the subscribers shall not be kept in Kamu SM since Kamu SM does not generate the subscribers' key pairs.

6.2.5. Private Key Archival

Kamu SM private keys shall not be archived.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

Transfer procedure is performed in encrypted form with reliable methods and under the supervision of several authorized personnel. During transfer, private key has been communicated to an unauthorized person or organization, then all certificates which are issued by the transferred private key are revoked.

6.2.7. Private Key Storage on Cryptographic Module

Kamu SM private keys are kept in encrypted form with secure algorithm and methods within secure cryptographic hardware device having FIPS 140-3 certificate, as blocked to access of unauthorized people. Transfer of private keys outside of the device has been blocked except for the backup purpose.

6.2.8. Activating Private Keys

Activation of Kamu SM private key is performed under the mutual supervision of several authorized personnel. Defined personnel should be available at the same time and identification and authentication should be electronically verified for the access to the room where the private key is available. In cases authorized personnel is not available in sufficient number and identifications are not verified, access may not be established for the room where the private key is available.

While private key is in the encrypted state within the cryptographic module, it is not in active state. Required data should be provided to the module for activation.

6.2.9. Deactivating Private Keys

Access to Kamu SM private key is automatically de-activated upon logging off the system and shall be logged off until following use. The method specified in Section 6.2.8 is operated for re-activation of the private key.

6.2.10. Destroying Private Keys

Kamu SM private key and all its backups are irreversibly destroyed with appropriate means upon their expiration, and these procedures are recorded. Authorized personnel in sufficient number as specified in Section 6.2.8 should be available at the same time for the procedure of destroying private keys and backups.

6.2.11. Cryptographic Module Capabilities

Kamu SM shall use a cryptographic module in compliance with the standards specified in Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

Public keys of Kamu SM and the subscribers are kept within the certificates and the certificates are archived according to procedures outlined in Section 5.5. Archives of the certificates are kept in an environment where required measures are taken against tampering and deleting by unauthorized people.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Usage period of private keys is as usage period of the certificate. Usage of private keys expires upon expiration of the certificate or revocation of the certificate. Usage period of key pairs of Kamu SM and the subscribers is determined according to key size and crypto algorithms used. Since 1 March 2018, the usage period of subscriber certificates cannot exceed 825 days and issued on or after 1 September 2020, the validity period is determined no greater than 398 days. Usage period of key pairs of Kamu SM may not exceed 30 years. The validity period of subscriber certificate cannot exceed the validity period of Kamu SM certificate.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

Activation data used within Kamu SM systems are generated in physically and electronically safe environments, blocked for access of unauthorized people, and having required complexity requirements.

Activation data are generated in compliance with the characteristics of the cryptographic module. Cryptographic modules used by Kamu SM minimum conform to FIPS 140-2.

6.4.2. Activation Data Protection

Access data used within Kamu SM are only used by authorized personnel. Required measures are taken in line with data protection policies of Kamu SM in the protection of these data.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

Required measures are taken against malicious software in Kamu SM. Intrusion detection system incorporating some network and server-based sensors is available in the system. Virus detection and cleaning agents that can be managed centrally have been installed on all servers and their update is continuously checked. Computers, where critical operations are performed, are excluded from the network. Required security measures are taken for ensuring protection against tampering, deletion, and leakage of information and maintaining operation. For all accounts that are authorized to certificate issuance, Kamu SM enforces multi-factor authentication. Copy of each installed software is backed up and all improvement actions for system security are implemented without delay. Security patches are not applied if they introduce additional vulnerabilities or instabilities and record based on risk assessment procedures. Network components and their configurations are periodically reviewed according to the network security procedure directive.

Authorizations not falling within the scope of the principle of separation of duties are not assigned in system infrastructure of Kamu SM. In this respect, periodic access review activities are performed. Required logging for all directly or indirectly certificate lifecycle related systems is performed.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

Controls are provided below while performing system development:

- Quality and security measures in sufficient level are taken.
- Personnel eligible for designated security criteria is employed.
- Copy of each installed software is backed up.

- All entities keeping system information is backed up for ensuring continuity of certification procedures.
- Required security measures are taken for connection of the system to the public network.
- The outsourced software is subject to virus scan before use and access of unofficial software to the system is blocked. All security requirements in this regard are fulfilled and all remedial actions are implemented without delay.
- System status is monitored closely at early stages for keeping up with possible abnormal system conditions.
- Access to the system being developed is performed by identifying information such as identity, password.
- Controls conducted during development of the system meet the requirements of the latest version of the standard of ISO 27001 Information Security Management Systems.
- Development, testing, and live systems are segregated during development activities. Go live procedure is performed following approval mechanisms.
- Periodic risk assessments in respect of system entities are conducted and submitted to management.
- Modifications performed in the systems are recorded and monitored.
- Access of third parties to the systems is not allowed including remote connections.
- Selection of third-party supplier in case of any consultancy or product requirement is performed based on previous references and work completion capabilities of the supplier.

6.6.2. Security Management Controls

Periodic security controls are performed for demonstrating that software and hardware products installed within the system and network environment functioning securely, as planned. Actions and authorizations not complying with security practices of Kamu SM are disclosed as a result of the audit and corrective actions are taken. A basis for security controls is the updated version of ISO 27001 Information Security Management Systems.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

Required network security controls are applied by considering the latest technological advancements. Protocols that are not required for the CA operations are blocked by firewalls. New generation firewalls equipped with intrusion prevention systems are used between internal and external networks. Network and system management infrastructures are available for the purpose of monitoring status and performances of servers and active devices in the system, issuing past performance reports and identifying future performance trends.

Network and system management and security agents are deployed on the servers. Management software retrieves the information such as a disk, memory, processor usage, file integrity, security log entries, external storage unit tracks etc. and monitor this information in real time. Threshold values are identified for sources that are of importance for the operation of servers and in case these

threshold values are exceeded, the system administrator is automatically alerted. Network and system management and security infrastructure stores such retrieved information in a central database. In this way, it enables to query data at any time and to issue past reports. If Kamu SM needs to communicate distinct trustworthy systems, Kamu SM establishes trusted channels which are logically distinct from other communication channels.

Different network segments have been issued for the high-security systems (such as root and subordinate CA servers). The systems where critical operations are performed are not connected to the network. Kamu SM's production systems for its services are separated from testing and development systems. Accessing secure zones and high secure zones are granted in accordance with the access control policy. Hardware that are used in high-security systems are not re-used in different places and they are destroyed.

Kamu SM also separates network for all employee groups such as IT admins, Software Developers, etc. Authorizations to privileged access accounts in the systems are provided by the security team in a controlled way and are monitored over log records. Communication and access to different areas are blocked, as well as non-essential connections and services are disabled for network security.

Security policy management practices are not used for different purposes. Unnecessary accounts, applications, services, protocols and ports in CA and SubCA systems are removed or disabled in accordance with the hardening procedure. All procedures regarding network and system security are monitored by the Cyber Incident Response Team (CIRT) and action is taken in line with incident response procedures, when necessary. To maintain continuity of the online services, the external network connection services of both the main center and disaster recovery center are redundant services.

Vulnerability scans are performed periodically on the systems and penetration testing is performed at least annually. The person/institution performing the penetration tests creates reliable reports that include the methods used in tests, the information about the tools used, the competencies/knowledge of the testers. These reports are recorded and kept in Kamu SM. Kamu SM reviews the established rule set on a regular basis.

6.8. TIME-STAMPING

Electronic records maintained for confidentiality, integrity, and availability of Kamu SM systems and services are kept as time stamped.

7. CERTIFICATE, CRL AND OCSP PROFILES

This section describes the profiles of certificates and CRLs issued, and structure of OCSP service provided by Kamu SM.

7.1. CERTIFICATE PROFILE

This section describes the contents of the root CA, subordinate CA and SSL certificates.

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” and “CA/Browser Forum

Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates". Certificate serial numbers are generated by using 64-bit entropy.

The contents of the root CA, subordinate CA and SSL certificates issued by Kamu SM are provided in Appendix-A.

7.1.1. Version Number(s)

Kamu SM supports the certificate standard of X.509 v3 in accordance with IETF RFC 5280.

7.1.2. Certificate Content and Extensions; Application of RFC 5280

The certificates issued by Kamu SM contain mandatory fields and X.509 v3 certificate extensions in accordance with IETF RFC 5280. Certificate extensions in the content of the certificate are determined depending on requirements of the application to be used by the certificate.

The contents of the root CA, subordinate CA and SSL certificates issued by Kamu SM are provided in Appendix-A.

Some of the extensions are defined as critical. In the event the extensions stated as critical fail to be defined by the application using the certificate, the certificate should not be used.

7.1.3. Algorithm Object Identifiers

"SHA-256 with RSA" algorithm (OID = {1 2 840 113549 1 1 11}) is used in signing all certificates, CRLs and OCSP responses issued by Kamu SM.

7.1.4. Name Forms

Name forms in the certificates issued by Kamu SM are specified in Section 3.1.1. Root CA, subordinate CA and SSL certificate name forms issued by Kamu SM are provided in Appendix-A. Kamu SM does not issue SSL certificates to IP Addresses and virtual or internal domain names.

7.1.5. Name Constraints

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.

7.1.6. Certificate Policy Object Identifier

The content of each certificate issued by Kamu SM contains an OID of relevant certificate policy for the purpose of specifying according to what certificate policy that certificate will be used. Kamu SM OV SSL OID (2.16.792.1.2.1.1.5.7.1.3) and CA/B Forum OV SSL OID (2.23.140.1.2.2) are used in SSL certificates issued by Kamu SM. Certificate Policy OID of the certificates issued by Kamu SM is provided under relevant certificate as set forth in Appendix-A.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

In the content of "Certificate Policy" extension in SSL certificates issued by Kamu SM, Kamu SM OV SSL is as set forth in Section 7.1.6 and policy qualifier value is http://depo.kamusm.gov.tr/ilke. Certificate Policy Qualifiers of the certificates issued by Kamu SM are provided under the relevant certificates as set forth in Appendix-A.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

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.

7.2.1. Version Number(s)

CRLs issued by Kamu SM conform to X.509 v2 format in accordance with IETF RFC 5280.

7.2.2. CRL and CRL Entry Extensions

The extensions defined in IETF RFC 5280 are used in CRLs issued by Kamu SM.

Extension	Value
CRL Number	Monotonically increasing integer
Authority Key Identifier	Subject Key Identifier in the certificate of CA signing CRL
Reason Code (Optional)	Reason for revocation

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".

7.3.1. Version Number(s)

OCSP service provided by Kamu SM supports v1 based on IETF RFC 6960.

7.3.2. OCSP Extensions

The extensions as set forth in IETF RFC 6960 can be used in OCSP service provided by Kamu SM.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This section provides information about the audit of Kamu SM compliance with its CP/CPS document.

8.1. FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

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 Security Management System audits conducted within the scope of ISO 27001 and internal audits conducted by reliable personnel.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor is selected from the qualified auditors accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403.

Assessors are competent people in the issue of the audit of public key infrastructure technology, information security and technology, and information systems. Assessors conduct their audits independently. ISO 27001 lead-auditor certificate is needed for ISO 27001 audits.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Assessors are the people independent from Kamu SM for not causing any conflict of interest and not damaging its independent entity.

8.4. TOPICS COVERED BY ASSESSMENT

During audits, certificate management procedures describing certificate management processes, security and functional controls of Kamu SM and their compliance with the CP/CPS document are audited.

Within this scope;

- Key and certificate lifecycle processes,
- CA system and environmental security controls,
- Processes compliance with the documents,
- Personnel competencies,
- Compliance with the principle of separation of duties,
- Compliance with CP/CPS, ISO 27001, ETSI EN 319 401, ETSI EN 319 411-1 and CA/B Forum the BRs are audited.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In cases where it is identified during the audit that Kamu SM fails to fulfill the requirements of the document of CP/CPS, the assessor notifies to the people concerned in a report it has issued in which processes the phases are not appropriate. Actions to be performed are identified and initiated for remedying identified deficiencies under the leadership of Kamu SM management.

In cases where it is identified that the requirements of CP/CPS are not duly fulfilled during installation, operation or maintenance phases of the system during the audit, the following actions shall be performed:

- Auditor notes down in which processes the phases are inappropriate and notifies relevant parties.
- Kamu SM remedies the deficiencies identified as a result of the audit in compliance with practice statement specified in CP/CPS document.
- In case of identifying a deficiency in critical procedures with respect to certificate management, Kamu SM suspends relevant processes until adjustments are duly made.

In cases where Kamu SM personnel creates fully or partially malicious electronic certificate, forges or falsifies electronic certificates issued validly, creates unauthorized electronic certificate or uses such electronic certificates on purpose and in case of other unauthorized actions, Kamu SM performs proceedings in pursuance of relevant legislation.

8.6. COMMUNICATION OF RESULTS

Audit results are communicated to Kamu SM management in report format. Kamu SM management ensures that the non-compliance set forth in the report must be corrected as soon as possible.

Audit reports are made publicly available within 3 (three) months through Kamu SM website.

8.7. SELF-AUDITS

Kamu SM checks compliance of SSL certificates with Certificate Policy and Certification Practice Statement by performing Kamu SM SSL self-audits. Kamu SM does self-audits on at least a quarterly basis against the full list of SSL certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal 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.

Under circumstances where the subscriber is not negligent such as theft, loss of private key of Kamu SM, breaching confidentiality or reliability of private key, modification of certificate policy or faulty generation of the certificate, certificates are revoked and renewed free of charge.

9.1.2. Certificate Access Fees

Kamu SM publishes its own certificate free of charge.

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees for Other Services

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 the repository.

9.1.5. Refund Policy

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

9.2. FINANCIAL RESPONSIBILITY

The Mandatory Liability Insurance and financial resource that Kamu SM must carry accordance with the law, will cover the loss unless CA fulfills its legal duties.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

Business plans, sales information, trade secrets and the information provided in non-disclosure agreements disclosed by Kamu SM and the parties receiving service are considered as business information. In addition, all documents not specifically reported as non-confidential are considered as confidential.

9.3.2. Information Not Within the Scope of Confidential Information

The information contained in all kinds of documents and certificates published in http://depo.kamusm.gov.tr/ website by Kamu SM is not considered as confidential.

9.3.3. Responsibility to Protect Confidential 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

9.4.1. Privacy Plan

Kamu SM maintains the privacy of personal/organizational information of the certificate applicants, the subscribers or other participants within the scope of the services provided thereon and they are all informed accordance with the law 6698 Personal Information Privacy Protection.

9.4.2. Information Treated as Private

Information such as demographic information, address information and phone numbers declared to Kamu SM for use within identification, authentication and certificate management procedures during application is treated as private.

9.4.3. Information Not Deemed Private

The information contained in the content of the certificate issued by Kamu SM is not confidential.

9.4.4. Responsibility to Protect Private Information

Kamu SM does not request information except required information for issuing the 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 the consent of the subscriber.

Required security measures are taken by Kamu SM for blocking unauthorized use and access to information required within the certificate life cycle during and after application of the subscribers. Only authorized personnel have access to the information of the subscribers.

Kamu SM provides information as part of Personal Data Protection Law on its website (www.kamusm.gov.tr/kurumsal/kvkk).

9.4.5. Notice and Consent to Use Private Information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

Kamu SM retains the intellectual property rights of all certificates and documents issued by Kamu SM and all information developed based on the CP/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.

9.6.1. CA Representations and Warranties

As an OV SSL provider, the representations and warranties of Kamu SM are as follows:

- Employing qualified personnel for required by the service,
- Executing certification procedures in compliance with policy and practice statements designated thereof,
- Publishing CP/CPS documents from public access repository,
- Generating key pairs for root and subordinate CAs and issuing certificates for these key pairs,
- Publishing root and subordinate CA certificates in environments accessible by end users,
- Identifying organization identity to issue the certificate based on official documents reliably,
- Performing authentication processes by way of duly accepting the certificate applications received from the government agency and by subjecting application forms with the documents of applicants to required controls, as set forth in Section 3.2.2,
- Ensuring the accuracy of the information in the content of the certificates based on the declared documents,
- Not issuing the certificate for applicant failed to meet required application requirements,
- Reviewing certificate applications and informing relevant governmental agency regarding the result of the application,
- Issuing certificate for the governmental agency whose certificate application has been accepted,
- Accepting certificate renewal applications as set forth in CP/CPS and performing required renewal procedures by way of reviewing process,
- Accepting certificate revocation applications as set forth in CP/CPS and performing required revocation procedures by way of reviewing process in a timely manner,
- In case it is identified that there is certificate usage not complying with CP/CPS document published and SSL Agreement, revoking the relevant certificate,
- Publishing revoked certificates information in CRL and announcing the same via OCSP service,

- Taking required measures to protect the integrity and the accessibility of the active and revoked certificates records uninterruptedly on a 24/7 basis,
- Taking required measures for protecting the confidentiality of the information of the subscribers kept electronically or in hard copy format, not disclosing such information to relying parties without the court order,
- Recording all procedures performed in relation to certificate generation, management, and revocation,
- Storing all hard copy and electronic records used during this process securely throughout the periods set forth in CP/CPS,
- Publishing root certificate according to legislation.

9.6.2. RA Representations and Warranties

Registration authority representations and warranties are as follows:

- Receiving certificate applications,
- Determining the identity information of the certificate applicant based on the required documents by the methods specified in this document,
- Receiving the required documents and information from the subscriber,
- Checking the “Subject” and “Subject Alternative Name” fields of the CSR,
- Delegating the verified certificate applications to the responsible units of Kamu SM,
- Delivering the SSL certificates to their owners,
- Receiving certificate revocation requests,
- Delegating the verified certificate revocation requests to responsible units of Kamu SM,
- Informing subscribers about revoked certificates.

9.6.3. Subscriber Representations and Warranties

Subscriber representations and warranties are as follows:

- Fulfilling the certificate application, revocation, and other procedures in compliance with the principle described in Kamu SM certificate management procedures as set forth in CP/CPS,
- Declaring accurate and complete information during certificate application and revocation procedures,
- Checking accuracy of the information contained in the issued certificate,
- Providing security of private key, in case of suspicion of losing confidentiality of private key, applying for Kamu SM as soon as possible for revoking the certificate,
- In cases where the content of the certificate issued by Kamu SM is modified, applying Kamu SM with immediate effect for revoking the certificate,
- Terminating of certificate usage in case of compromising of the private key,
- Communicating with Kamu SM when the modifications occurred in declared information during the certificate application and validity period of the certificate,
- Performing no actions with revoked or expired certificates,

- Not using the certificate in the domain other than specified in the issued certificate,
- Not using its private key for the purpose of signing a subordinate CA certificate,
- Using the certificate issued to itself as set forth in CP/CPS document and within the conditions stipulated in SSL Agreement.

In cases where relying parties suffer a loss by virtue of the breach of the representations and warranties revealed hereinabove, TÜBİTAK reserves the right to recourse the compensations it has to pay to the subscriber.

9.6.4. Relying Party Representations and Warranties

Relying parties are liable for performing validity checks of the certificate provided below before performing any action relating to the certificate:

- Verifying that the certificate is used in compliance with its intended purpose of issuance,
- Checking expiration period of the certificate,
- Checking the validity of the certificate via CRL or OCSP service,
- Verifying integrity of revocation status record obtained from CRL or OCSP service by using public key existing within relevant certificates of Kamu SM,
- Verifying authenticity of the certificate using public key existing within subordinate CA certificate of Kamu SM,
- Verifying authenticity of subordinate CA certificate of Kamu SM by using public key existing within root certificate,
- Verifying authenticity of root certificate of Kamu SM by checking certificate hash value,
- Verifying that the subscriber possesses private key corresponding to the public key within the certificate.

9.6.5. Representations and Warranties of Other Participants

Other participants consisting of all people and organizations that Kamu SM procures service while offering OV SSL Certificate service warrant that they shall offer the said service in the most diligent manner and they shall not disclose confidential or private information relating to its customers and the procedures of Kamu SM. Service contracts wherein warranties are explicitly stated between the people or organizations that Kamu SM has procured service will be duly executed.

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 the 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/CPS document throughout the period where they receive certificate services.

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

9.10.1. Term

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

9.10.2. Termination

SSL Subscriber Agreement may be terminated in the following circumstances:

- Revocation of the certificate by the subscriber,
- Expiration of the certificate,
- In cases where the subscriber acts in contradiction with Subscriber Agreement, revocation of the certificate of the subscriber by Kamu SM,
- Revocation of the certificate of the subscriber by Kamu SM due to the emergence of security breach specified in Section 5.7.3,
- If Kamu SM terminates certificate services as set forth in Section 5.8, revocation of the certificate of the subscriber by Kamu SM.

9.10.3. Effect of Termination and Survival

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

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

Even if agreements expire, Kamu SM continues to fulfill its liabilities in relation to the certificates it has issued thereto. Kamu SM maintains its services relating to ensuring access to issued certificates and revocation status records by the parties, storage of the records and archives set out in Section 5.4 and 5.5.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Kamu SM notifies the subscriber regarding result of certificate application in certification administration procedures and the result of revocation and renewal requests. Notices will be made via

phone, fax or e-mail. Notifications made to an e-mail of the agency specified in certificate application form, if modified, to a newly notified e-mail address will be considered as official notification.

Notifications relating to the procedures deemed critical as regards certificate management will be made in writing.

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

9.12.1. Procedure for Amendment

CPS document has been written by Kamu SM. Amendments likely to be made on the CPS document may be either by way of addition or modification or Kamu SM may decide on the whole renewal of the document. Even if it is revealed that any part of the CPS document is inaccurate or invalid, other parts of the CPS document of Kamu SM will survive until the CPS document is updated.

9.12.2. Notification Mechanism and Period

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

9.12.3. Circumstances under Which OID Must Be Changed

No stipulation.

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, 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.

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 CP/CPS document are found to be in contradiction with the relevant legislation to be effective thereafter, required adjustments shall be made and duly adapted.

9.16. MISCELLANEOUS PROVISIONS

No stipulation.

10. APPENDIX-A CERTIFICATE PROFILES

10.1. ROOT CA CERTIFICATE OF KAMU SM

Area	Value
Version	V3
Serial Number	01
Signature Algorithm	RSA with sha-256 {1 2 840 113549 1 1 11}
Issuer	CN = TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR
Valid From	25 November 2013 Monday 11:25:55
Valid To	25 October 2043 Sunday 11:25:55
Subject	CN = TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR
Subject Public Key	2048 bit RSA {1 2 840 113549 1 1 1}
Area	**Value**
Subject Key Identifier	Critical=No; 65 3f c7 8a 86 c6 3c dd 3c 54 5c 35 f8 3a ed 52 0c 47 57 c8
Key Usage	**Critical=Yes**; Certificate Signing, Offline CRL Signing, CRL Signing
Basic Constraints	**Critical=Yes**; Subject Type=CA; Path Length Constraint=None

10.2. SUBORDINATE CA CERTIFICATE OF KAMU SM

Area	Value
Version	V3
Serial Number	29
Signature Algorithm	RSA with sha-256 {1 2 840 113549 1 1 11}
Issuer	CN = TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR
Valid From	14 May 2015 Thursday 16:32:27
Valid To	11 May 2025 Sunday 16:32:27
Subject	CN = TUBITAK Kamu SM SSL Sertifika Hizmet Saglayicisi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR
Subject Public Key	2048 bit RSA {1 2 840 113549 1 1 1}
Area	**Value**
Authority Key Identifier	Critical=No; 65 3f c7 8a 86 c6 3c dd 3c 54 5c 35 f8 3a ed 52 0c 47 57 c8
Subject Key Identifier	Critical=No; f6 35 35 17 ae 2e fb b7 7d f7 76 17 8a 65 64 eb 67 7a 40 ab
Key Usage	**Critical=Yes**; Certificate Signing, Offline CRL Signing, CRL Signing
Basic Constraints	**Critical=Yes**; Subject Type=CA; Path Length Constraint=0
Certificate Policy	[1] Certificate Policy: Policy Identifier= All issuance policies [1.1] Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier=http://depo.kamusm.gov.tr/ilke/ [1,2] Policy Qualifier Info: Policy Qualifier ID=User Notice Qualifier= Notice Text=Bu sertifika ile ilgili Sertifika Ilkelerini okumak için belirtilen web sitesini ziyaret ediniz.

CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://depo.kamusm.gov.tr/ssl/SSLKOKSIL.S1.crl
Authority Information Access	[1] Authority Information Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Other Name: URL= http://depo.kamusm.gov.tr/ssl/SSLKOKSM.S1.cer [2] Authority Information Access Access Method= Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Other Name: URL= http://ocspsslkoks1.kamusm.gov.tr

10.3. SUBSCRIBER SSL CERTIFICATE TEMPLATE

Area	Value
Version	V3
Serial Number	An integer containing 64 bit random number
Signature Algorithm	RSA with sha-256 {1 2 840 113549 1 1 11}
Issuer	CN = TUBITAK Kamu SM SSL Sertifika Hizmet Saglayicisi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR
Valid From	Certificate generation time
Valid To	End of certificate validity
Subject	CN = <CommonName> O = <Organization> OU = <OrganizationalUnit> (Optional) ST = <StateOrProvince> L = <Locality> (Optional) C = TR
Subject Public Key	RSA/ECC

Extensions	Value
Authority Key Identifier	Critical=No; f6 35 35 17 ae 2e fb b7 7d f7 76 17 8a 65 64 eb 67 7a 40 ab
Subject Key Identifier	Critical=No; Includes the SHA-1 hash output of the "BIT STRING" value of "subjectPublicKey" field of the certificate.
Key Usage	**Critical=Yes**; Digital signature, Key Encipherment
Basic Constraints	Critical=No; Subject Type=Subscriber; Path Length Constraint=None
Certificate Policy	[1] Certificate Policy: Policy Identifier=2.16.792.1.2.1.1.5.7.1.3 [1.1] Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier= http://depo.kamusm.gov.tr/ilke [2] Certificate Policy: Policy Identifier=2.23.140.1.2.2
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://depo.kamusm.gov.tr/ssl/SSLSIL.S1.crl
Authority Information Access	[1] Authority Information Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Other Name: URL= http://depo.kamusm.gov.tr/ssl/SSLSM.S1.cer [2] Authority Information Access Access Method=Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Other Name: URL=http://ocspssls1.kamusm.gov.tr
Subject Alternative Name	DNS Name=<Domain Name 1> DNS Name=< Domain Name 2> ... DNS Name=< Domain Name n>