SSL CERTIFICATE POLICY AND CERTIFICATE PRACTICE STATEMENT

Document Code	Issue Number	Date of Issue
YONG-001-009	**03**	**19.12.2015**

MODIFICATION LOGS

Issue No	Reason of Issue	Date of Issue
01	First issue.	05.12.2007
02	Modifications were made regarding RSA 1024-bit certificates. Minimum key length was regulated as RSA 2048-bit.	24.02.2009
03	Modifications were made regarding deployment of the new SHA-256 Sub CA	19.12.2015

CONTENTS

1. Introduction

This is a Certificate Policy and Certificate Practice Statement (CP/CPS) document defining the principles implemented by Government Certification Authority (Kamu SM) formed by Informatics and Information Security Research Center (BİLGEM) of TÜBİTAK (The Scientific and Technological Research Council of Turkey) while providing SSL certificate service.

Government Certification Authority (Kamu SM) provides the functions of Certificate Authority (CA) as defined at Electronic Signature Law, the Regulation on the Application Methods and Principles of Electronic Signature Law No. 5070 and dated Jan., 15th, 2004 issued by the Telecomunication Institute and the Annunciation on the Procedures and Technical Criteria for Electronic Signature.

The people who demand a SSL certificate from Kamu SM accept the certificate within the framework of the principles in this document. The certificates given to equipments are not considered as the qualified electronic certificates mentioned at Electronic Signature Law No. 5070.

1.1. Overview

CP/CPS document defines the roles, responsibilities and relations of the system components in the Kamu SM and tells how the certificate management and registration transactions are done. Certificate management consists of actions such as creation of key pairs and certificates for certificate owners, to renew, ~~to update,~~ to suspend and to revoke certificates, to issue the information of certificate revocation, certificate transactions and to inform the relevant people about the application and the position of the certificate, to keep the necessary registrations and make the registration transactions. Registration transactions consist of receiving the applications, ID information and the public documents of the people or organizations who demand the certificate, to receive their demands on approval, revocation, renewal to evaluate them and to start the necessary transactions of the approved certificates and revocation of the certificates.

CP/CPS document has been referred to IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) and the expression “Has not been deemed necessary to regulate" under some subheadings placed as embedded herein the document means that no arrangement has been done as no necessity considered at this stage.

1.2. Document Name and Identificatiom

Document Name: SSL Certificate Policy and Certificate Practice Statement

Document Version Number: 03

Published On: 19.12.2015

OID: 2.16.792.1.2.1.1.5.7.1.2

1.3. PKI Participants

1.3.1. Certificate Authorities

Kamu SM provides SSL certificate service as Electronic Certificate Service Provider. It provides the following services for this reason.

- Generation and signing of certificates and delivery to related persons or organizations
- Revocation of certificates
- Issuing the certificate status information in form of Certificate Revocation List (CRL) or by other methods

1.3.2. Registration Authorities

Has not been deemed necessary to regulate.

1.3.3. Subscribers

Natural or legal persons, for whom certificates are generated by Kamu SM and who are obliged to use their certificates in accordance with the principals and implementation rules of Kamu SM certificate.

1.3.4. Third Parties

They are the people who accept and make transactions relying on the fact that the link between the ID information and the signature verification data of the certificate generated by Kamu SM are true. Third parties control the necessary validity before using the certificate when they think it is necessary.

1.3.5. Other Participants

Has not been deemed necessary to regulate.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Usage

SSL certificates are used in order to realize the act of authentication between the server and client systems and to allow the communication as encrypted.

1.4.2. Prohibited Certificate Usage

The SSL certificates generated by Kamu SM cannot be used for purposes other than those specified in Article 1.4.1.

1.5. Policy Administration

1.5.1. Document Management

This CP/CPS document has been written by Kamu SM. Kamu SM may change the document when it considers necessary.

1.5.2. Contact Details

Questions about the implementation and the related management principals about this CP/CPS document can be directed to the access points of TÜBİTAK-BİLGEM below:

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

Phone : 444 5 576
Fax : (262) 648 18 00
E-mail : bilgi@kamusm.gov.tr
URL : http://www.kamusm.gov.tr

Kamu SM issues CP/CPS document at the web address below, which is accessible by anyone:

http://depo.kamusm.gov.tr/ilke

1.5.3. Person Determining the CP Suitibility for the Policy

The convenience of this CP/CPS document is determined by the management of Kamu SM and the people authorized by the management.

1.5.4. Approval Procedures of Certificate Practice Statement

The approval for the issue of this CP/CPS document is determined by the management of Kamu SM and the people authorized by the management.

1.6. Definitions and Abbreviations

1.6.1. Definitions

Key pair: The private key, used to create and verify an electronic signature or to encrypt and decrypt a data and the related public key.

Information storage: Data storage contexts like the index servers where information about the certificates, certificate revocations and other certificate transactions are issued.

SSL Certificate Authority: Certificate Authority which was formed within the Kamu SM, which has the certificate that bears the signature of the SSL Root Certificate Authority and which is authorized to create the SSL certificates of the users and sign them.

Online certificate status protocol: The standard communication rule which allows the people to learn their certificate revocation status by demanding the control of certificate validity as an alternative to the third party's certificate revocation list.

Revocation status record: A record where the revocation information of the certificates of which usage deadline is not due, which enables to define the exact revocation time and a record where the third parties may easily reach.

Government Certification Athority: A division formed for electronic certificate services within the body of Informatics and Information Security Research Center (BİLGEM) of TÜBİTAK (The Scientific and Technological Research Council of Turkey).

SSL Root Certificate Authority: The Certificate Authority which signs its own certificate and is the highest authority in signing certificates, formed within the body of Kamu SM.

Object authentication number: A number that defines an object as "unique" and is taken from an institution which sets the international standards.

Certificate update: The process of giving new certificates to people who don't have certificates at the moment, but who are registered in the system as certificate owners.

Certificate revocation list: A file which contains the information of revoked certificate data and has the signature of CA.

Certificate owner: A real or legal person who gets a certificate from Kamu SM.

Certificate renewal: The process of giving new certificates to people who have valid certificates at the moment and are registered in the system as certificate owners.

End-users: The certificate owners and the third parties who use the certificates.

Third parties: Real or legal entities that carry out transactions relying on the certificates.

Time stamp: A record verified by CA with an electronic signature in order to confirm when an electronic data was generated, changed, sent, received and/or recorded.

1.6.2. Abbreviations

BS: British Standards

CA: Certification Authority

CEN (Comité Européen de Normalisation): European Standardization Committee

CP: Certificate Policy

CPS: Certificate Practice Statement

CRL: Certificate Revocation List

CWA: CEN Workshop Agreement

DSA: Digital Signature Algorithm

DSA Elliptical Curve: Digital Signature Algorithm Elliptical Curve

EAL: Evaluation Assurance Level

ETSI: European Telecommunications Standards Institute

ETSI TS: ETSI Technical Specification

FIPS PUB: Federal Information Processing Standards Publications

IETF RFC: Internet Engineering Task Force Request for Comments

ISO/IEC: International Organisation for Standardisation / International Electrotechnical Committee

ITU: International Telecommunication Union

Kamu SM: Kamu Sertifikasyon Merkezi (Government Certification Authority of Turkey)

LDAP: Lightweight Directory Access Protocol

OCSP: Online Certificate Status Protocol

PKI: Public Key Infrastructure

RSA: Rivest Shamir Adleman (The Initials of the surnames of the people who invented the Algorithm)

SHA: Secure Hash Algorithm

SSL: Secure Sockets Layer

2. Publication and Repository Responsibilities

Repository is the continuous, safe and free broadcast medium where the certificates that the Kamu SM create, the revocation state logs, and the related documents such as SI and SUE are stored allowing the access of certificate owners and third parties.

Kamu SM's repository is reached over the Internet. Information about Kamu SM, documents relating the certificate management, technical information documents, application forms and announcements are issued over the Internet.

2.1. Repositories

Kamu SM uses the services on the Internet as repository. The addresses of the repository and the accessible information are defined below.

CP and CPS documents can be reached at http://depo.kamusm.gov.tr/ilke.

CRLs and certificates belonging to Kamu SM can be reached at the web address http://depo.kamusm.gov.tr.

As an alternative to the certificate revocation lists, the most up-to-date validity states of the certificates can be verified over the OCSP Responders operating at http://ocspces4.kamusm.gov.tr and http://ocspkok3.kamusm.gov.tr.

2.2. Publication of Certification Information

The following information is stored in the repository that the Kamu SM will provide access to the system elements, with the exception of the information about its internal operation:

- Root CA and Subordinate CA certificates of Kamu SM,
- The hash value of the Root CA and Subordinate CA certificate of the Kamu SM, and the information about the hash algorithm used in the calculation of the hash value.
- Kamu SM CP and CPS documents,
- Commitment letters,
- Forms,
- CRLs

2.3. Time and Frequency of Publication

Commitment Letters, Certificate Contracts, procedures of managing the SSL certificates, CP and CPS documents are updated as the content changes. Updated documents are released immediately after the update.

Certificates of Kamu SM are issued immediately after the update.

The issuing frequency of CRL's is stated in Chapter 4.9.7 and 4.9.9 of this document.

2.4. Access Controls

Everyone is allowed to access the repository of Kamu SM for information purposes.

The updating of the repository is performed by the authorized Kamu SM personnel.

Kamu SM carries out the following responsibilities in accordance with the repository:

- Ensuring the integrity of the information stored in the repository against unauthorized deletion and editing,

- Ensuring the accuracy and actuality of the information stored in the repository,
- Keeping the repository accessible,
- Taking necessary precautions for providing continuous access to the repository,
- Providing the free access to the repository.

3. Identification and Authentication

3.1. Naming

3.1.1. Type of Names

In certificates created by Kamu SM, the name types supported by "ITU X.500" format are used in the DN (Distinguished Name) domain, where the credentials of certificate owners, are defined.

3.1.2. Need for Names to be Meaningful

The ID information on the certificates has to be meaningful so as to identify the real or legal bodies (name, surname, organization name, mail address).

3.1.3. Use of Alias or Nickname by Certificate Owner

The certificate owner is not allowed to use nicknames or aliases within the context of his certificate.

3.1.4. Interpreting Different Name Forms

No name space other than ITU X.500 form can be used in the certificates.

3.1.5. Uniqueness of the Names

The credentials embedded in the certificates generated by Kamu SM are unique for each user. However, using the same credentials for different electronic certificates of the same natural person or legal person is allowed. It is prohibited to utilize the same credentials in the electronic certificates of different natural person or legal person.

3.1.6. Identification, Authentication and Role of Trademark

The applicants of certificates cannot use such names that may harm the intellectual and industrial property rights of others during the time of application. It cannot be verified whether the intellectual and industrial property rights of the names used during the time of application belong to applicants. Regarding any intellectual and industrial property right problem that may occur, the Kamu SM has the right to reject the certificate application or revoke the generated certificates. Kamu SM shall not execute any reconciliation oriented to the troubleshooting of such problem.

3.2. Initial Identity Validation

The following methods are used for authenticating the credentials of the related person or organization upon the initial application for using the Kamu SM certificate services.

3.2.1. Proving Possession of Signature Creation Data

During the SSL Certificate application, the certificate signing inquiry created by the applicant, is signed with the signature creation data. Therefore the ownership of signature creation data is verified.

3.2.2. Authentication of Corporate Identity

The ID determination of public organizations that have demanded for SSL certificate from Kamu SM shall be carried out by official correspondence between Kamu SM and related

public organizations and verification of field name specified in the certificate signing inquiry through relevant channels (nic.tr).

3.2.3. Authentication of Personal Identity

It is verified as described in article 3.2.5 whether the persons inquiring SSL certificate from Kamu SM are authorized to demand certificates regarding the domain name to appear on the certificate.

3.2.4. Unverified Subscriber Information

The SSL certificates generated by Kamu SM do not contain unverified information.

3.2.5. Verification of Authority

It is verified by official correspondence between Kamu SM and related public organizations whether the persons inquiring SSL certificate from Kamu SM are authorized to demand certificates regarding the domain name on the certificate.

3.2.6. Criteria for Interoperation

Has not been deemed necessary to regulate.

3.3. Identification and Authentication for Certificate Renewal Request

3.3.1. Identification and Authentication for Routine Certificate Renewal Request

Certificate owners with a valid certificate may apply to Kamu SM for an ordinary certificate renewal request, before the expiration date of the certificate and if no changes has been made to the contents of the certificate. For the usual certificate renewal request, authentication is carried out as described in 3.2.2 and 3.2.3

3.3.2. Identification and Authentication on Certificate Update Request after Revocation

In cases that the information stored within the certificate changes, the certificate expires and an application for a new certificate after revocation is made, the certificate owner requests for an update. For the post-revocation certificate renewal request, authentication is carried out as described in 3.2.2 and 3.2.3

3.4. Identification and Authentication for Certificate Revocation Request

The certificate owner may request the revocation of his/her certificate sending a printed form or letter with signature on it to Kamu SM.

For the revocation appeals served by original signed papers or letters, the authentication is carried out by communicating the certificate owner via his contact information.

4. Certificate Life-Cycle Operational Requirements

In this Chapter, the operations in the certificate administration processes are described. The details of the processes are stated on Kamu SM's web site. The certificate administration is composed of the following processes:

- Certificate application
- Certificate renewal
- Certificate update
- Certificate revocation

The processes include the operations performed between the certificate owners and Kamu SM.

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

The application for SSL certificates is made institutionally by the organizations or corporations to Kamu SM. The organization signs the SSL Commitment Letter and SSL Request Form, which states the conditions of the certificate services provided by Kamu SM. An employee cannot apply for a certificate in person without the approval of the organization.

4.1.2. Registration and Responsibilities

The application for SSL certificates is made by the organizations or corporations to Kamu SM. The organization signs the SSL Commitment Letter and SSL Request Form, which state the conditions of the certificate services provided by Kamu SM and send them to Kamu SM.

The organization sends the certificate signing request necessary for the SSL certificate to Kamu SM from the corporate e-mail address.

4.2. Processing the Certificate Application

4.2.1. Performing Identification and Authentication Processes

The operations of identification and authentication are performed upon the evaluation of the documents delivered during application, by Kamu SM.

The organizations applying for SSL certificate convey to Kamu SM the official letter and SSL certificate application forms as attached therewith. Whether the organization has the right to use the domain name record on the related form is check through the TR domain name management.

4.2.2. Approval or Denial of the Certificate Application

As a result of the controls stated in the Chapter 4.2.1, the application is denied if any falsifications, errors, missing approvals, or inaccurate information is detected on the documents submitted during the certificate application. The organization and/or the applicant are informed orally or in writing about the rejected applications. Written notification is performed by sending an e-mail to the organization and/or to the applicant. Verbal notification is performed by calling the organization and/or the applicant. The email addresses and the phone numbers of the organization and the applicant are the information stated during

the application. The application may be repeated once the necessary corrections are made and the deficiencies are corrected.

The approved applicants are defined in the Kamu SM system and the process of certificate generation is started.

4.2.3. Processing Time of Certificate Application

The certificate application is processed and resulted in 3 (three) working days at most upon the receipt of all the necessary and valid documents by Kamu SM.

4.3. Certificate Generation

4.3.1. Functions of CA in Certificate Generation

Kamu SM generates the certificates on behalf of the real and legal persons whose certificate applications have been completed and who have been identified as users in the system. Before generating the SSL certificate, it is also checked whether the certificate signing request that the applicant has conveyed to Kamu SM provides the technical criteria or not.

4.3.2. Notifying the Certificate Owner about the Certificate Generation

Kamu SM sends the generated SSL certificate to its owner's corporate e-mail address.

4.4. Acceptance of the Certificate

4.4.1. Way of Activating the Certificate

From the moment the SSL certificates are delivered to certificate owners, same are deemed to be accepted by the owners. The certificate owner controls whether the information on the certificate is the same as those that he declared during the application and in case of any non-compliance, promptly notifies Kamu SM and avoids using the certificate. The certificate is revoked by Kamu SM.

4.4.2. Publication of the Certificate by the CA

Kamu SM does not publish the generated SSL certificates.

4.4.3. Notifying Other Entities about Certificate Generation

Has not been deemed necessary to regulate.

4.5. Key Pair and Certificate Usage

4.5.1. Usage of Certificate and Signature Creation Data by Certificate Owner

Certificate owners are liable to protect the signature creation data against any access by unauthorized persons. The signature creation data corresponding to the SSL certificates can only be used for the purposes specified in "Key Usage" field on the certificate.

4.5.2. Usage of Certificate and Signature Verification Data by Relying Parties

The signature verification data in the certificate owner's certificate are used by the third parties for purposes of verification. Third parties are liable to control the validity of the CA certificate generating the certificate to rely on, to verify that such certificate is used within the "Key Usage" of the certificate and to comply with the conditions of use specified in these CP/CPS documents.

4.6. Certificate Renewal

Certificate renewal means renewal of the certificate using the old key pair. This process is not allowed in the Kamu SM systems.

4.7. Certificate Re-key

Certificate renewal is the generation of a new certificate that will take place of the old certificate, for the certificate owner who already owns a valid certificate in the system, by generating a new key pair, without changing any of the information stored in the certificate, before the expiration date of the certificate. No certificate renewal is practiced for SSL certificates. Should the certificate owner wish to re-appeal for certificate, he practices such appeal as described in chapter 4.1.

4.8. Certificate Modification

In the events of expiry of the validity term of the certificate or any change of information within the content of the certificate, "certificate update" shall mean the inquiry of a certificate again and generation of the same. The certificate update is assessed within the scope of new certificate appeal and the procedure in chapter 4.1 is implemented.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Certificate Revocation

The revocation of certificate is the process of canceling the certificate that loses the validity before the expiration date. The cancellation of the certificate implies the notification of the public about the revocation.

The certificate owner requests the revocation of the SSL certificate under the following conditions:

- Being skeptical about the security of the signature creation data,
- Occurrence of changes in the information stored in the certificate.

Kamu SM cancels the certificate of the certificate owner if any one of the following conditions occurs:

- Detection of false or faulty information about the certificate owner in the certificate,
- Utilization the certificate inconsistently with the Commitment Letter and violating the conditions stated in the CP/CPS documents,
- A breach in the security of the signature creation data used by Kamu SM to sign the certificates,
- Kamu SM stopping its activities and another CA not being able to provide the continuance of the administration of the provided SSL certificates.

4.9.2. Who Can Submit for Revocation

The organization executive who bears the domain name has the revocation entitlement of SSL certificate granted by Kamu SM. Kamu SM performs the authentication actions before revoking the certificate.

Kamu SM has the authorization to revoke the certificate under the conditions described in Chapter 4.9.1. Kamu SM informs the certificate owner of the revocation reason.

4.9.3. Processing the Certificate Revocation Application

The appeal of revoking the SSL certificate may be tendered by the domain name bearing organization to the Kamu SM by approved official letter notice.

The directions for revocation applications are described in detail at Kamu SM's web address http://www.kamusm.gov.tr. Kamu SM continuously provides the services necessary to perform the revocation process.

Kamu SM processes the revocation information and announces to the public as soon as possible. The revocation announcements made to the public includes at least the serial number of the certificate and Kamu SM's electronic signature. Kamu SM announces the revocation status records by issuing CRL for the SSL certificates and in addition, by setting the state of certificates to revoke position at OCSP Responder.

CRL file is signed by Kamu SM's signature creation data. Serial numbers of the revoked certificates are kept in CRL until expiration. The certificate serial number is removed from CRL when it expires. The status of the revoked certificates will continue to appear as revoked on OCSP Responder until they expire.

4.9.4. Revocation Request Grace Period

No such projection has been made.

4.9.5. Processing Time for Revocation Request

Kamu SM immediately processes the valid revocation requests and revokes the certificate after the necessary authentication.

4.9.6. Necessity to Control the Certificate Revocation Status by Third Parties

Kamu SM opens the revocation status records to public free of charge. Everyone can access the certificate revocation status records without the necessity to authenticate the querrier. Kamu SM provides continuous access to the revocation status records.

Third parties are responsible for checking the validity of the certificate using either one of CRL or OCSP methods before processing any operations with the certificates.

Third parties check whether the revocation status record provided by CRL file or OCSP Responder is signed by Kamu SM's signature creation data, during the validation of the certificate. The validity checks that third parties have to perform are stated in chapter 9.6.4.

4.9.7. CRL Issuing Frequency

The validity period of CRL, where the certificate revocation information is stored, is 36 (thirtysix) hours. However, CRL is updated 23 (twentythree) hours after the issuing time without waiting until the end of this period. CRL is updated even though there has not been a new certificate revocation within the same day. The old CRL files will remain valid until their expiration.

The CRL file that includes the revocation information about Kamu SM's sub root certificates is updated in every 10 (ten) months. The CRL file will immediately be updated on a certificate revocation.

4.9.8. CRL Latency

The CRL will be issued in max 5 (minutes) after the announced issuing time.

4.9.9. Support for Online Certificate Revocation Status Record

Kamu SM issues the SSL certificates revocation status information over OCSP. The revocation status records issued on OCSP are signed by the signature creation data of Kamu SM. The revocation status records on OCSP Responder is updated in 30 (thirty) seconds following the receipt of the revocation request.

The applications with OCSP support perform the validation of the SSL certificate over http://ocspces4.kamusm.gov.tr and and the validation of the sub CA certificate over http://ocspkok3.kamusm.gov.tr.

4.9.10. Requirement for Online Certificate Revocation Status Record

Kamu SM provides the online certificate revocation status record support along with CRL, as the online method adds less load on the system and provides the most recent data.

CRL file is an incrementally growing file as the revocation information for each and every revoked certificate is added to this file. The file must be downloaded from the Kamu SM repository every time the updated revocation status record is required. In contrary with the ever-growing CRL file and the load it adds to the system, OCSP allows the querying the revocation status of the related certificate in a question and answer methodology.

4.9.11. Other Certificate Status Notification Methods

Kamu SM performs no other methods of certificate status notification but CRL and OCSP.

4.9.12. Security Breach in Signature Creation Data

The certificate is revoked in case of a breach in the security of the signature creation data. No other actions are taken in such cases.

4.9.13. Conditions for Certificate Suspension

No suspension process is applicable for SSL certificates.

4.9.14. Persons Qualified for Certificate Suspension Application

Has not been deemed necessary to regulate.

4.9.15. Processing the Certificate Suspension Request

Has not been deemed necessary to regulate.

4.9.16. Suspension Duration

Has not been deemed necessary to regulate.

4.10. Certificate Status Services

Third parties may access the Kamu SM certificate revocation status records via CRL and OCSP services as stated below.

4.10.1. Operational Features

The third parties may access the certificate revocation status records by the CRL files of Kamu SM. The access information on the CRL files of Kamu SM is defined in Chapter 2.

The third parties copy the updated CRL file from Kamu SM repository to their systems whenever they wish to check the revocation status record and perform the necessary controls.

The third parties with OCSP Client support can check the certificate revocation status over OCSP Responder. The access address for OCSP Responder is stated in Chapter 2. The third parties run a query on OCSP Responder whenever they wish to check the validity status of the certificate(s).

4.10.2. Availability of the Service

All the precautions necessary for providing uninterrupted access to the systems running CRL and OCSP services are taken by Kamu SM. Nevertheless, if the access is interrupted temporarily, the third parties shall stop their activities of checking the certificate revocation status record until the problem is fixed. Kamu SM shall not be held responsible for the losses arising from the transactions made without checking the revocation status records due to the interruption in system access.

4.10.3. Optional Features

Has not been deemed necessary to regulate.

4.11. Termination of the Certificate Ownership

The certificate ownership is terminated as the certificate expires, revoked, and as Kamu SM stops its certificate services. Kamu SM informs the certificate owner and other parties if stated in the commitment letter, in cases that the certificate is revoked and that Kamu SM stops its certificate services. In case of expiration, Kamu SM does not notify the certificate owner; the certificate owner is obliged to follow up the expiration date of his certificate.

4.12. Key Escrow and Recovery

The keys of the certificate owners are not recovered or backed up.

5. Facility, Management and Operational Controls

In this Chapter, the non-technical security controls to be performed during the certificate service provided by Kamu SM are described.

5.1. Physical Controls

The buildings and the rooms where the Kamu SM systems operate are equipped with the security precautions such as access control systems that avoid unauthorized access.

5.1.1. Site Location and Construction

The building where the Kamu SM systems operate is located away from the residential areas, at a location where the disasters such as fire, flood, earthquake, lightning and air pollution have a minimal impact, and the access to the area is controlled.

The building is suitable for the high-security operations. The building fulfills the structural conditions of flexibility (steel construction) and hard (steel reinforced concrete construction).

There are power supplies, communication units, ventilations and fire distinguishers within the place and the building where Kamu SM is located, and the necessary precautions are taken against earthquakes, flood and other disasters.

5.1.2. Physical Access

The access to the Kamu SM software and hardware modules, as well as the archives, is controlled. The access to the building is under control of the security officers, supported with advanced access control devices.

The access to the rooms where the software and hardware of the Kamu SM systems are located, the soft or hard copies of the information are stored, as well as the operation and administration rooms are controlled with advanced access control devices. Unauthorized personnel cannot access to the system rooms. The access of the unauthorized personnel to the system-related rooms for maintenance or similar extraordinary reasons is regulated by special access instructions.

5.1.3. Power Supply 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 the necessary ventilating system.

5.1.4. Water Exposures

The necessary precautions to minimize the damages arising from the floods are taken at the locations where Kamu SM operates.

5.1.5. Fire Prevention and Protection

The necessary precautions to prevent fires and to minimize the damages of possible fire events are taken at the locations where Kamu SM operates.

5.1.6. Protection of Storage and Backup Media

The data storage media (discs, CDs, paper, etc.) are protected physically and electronically against corruption and aging.

5.1.7. Termination of Wastes

The obsolete electronic media and papers, where sensitive information are stored, are terminated irreversibly.

5.1.8. Backing up at Different Locations

CA keeps the components which seem necessary fort he continuation of the system in different places and in safes. The place, where the backup system is located, complies with all safety and functionality conditions of the main system.

5.2. Procedural Controls

5.2.1. Trusted Roles

The roles of the personnel in Kamu SM are classified as below:

Kamu SM Administrator: Ensures the internal operations of Kamu SM, the compliance with the laws, the compliance with the directions and policies, and makes the necessary modifications and regulations when required.

Kamu SM Technical Manager: Ensures the technical harmony between the units of KamuSM. Examines the technical activities. Monitors the security and performance of the information technologies.

Security Manager: Monitors the application of the security methods and policies of KamuSM. Detects the security needs of the system over time and coordinates the satisfaction of such needs.

Security Operator: The operator is responsible for providing the border security and the operation of the related assets. Ensures the operation of firewalls, intrusion detection system, logging system and antivirus systems.

System Administrator: Responsible for operation of all the system with the exception of the security components. Coordinates the modifications to be made in the system over time.

System Operator: Responsible for the operating system and hardware of all servers. Makes the necessary updates of the related components.

Data Systems Administrator: Manages the directories and the database clusters. Manages the database activities.

Certificate Process Administrator: Makes suggestions on updating or modifying the CP and CPS, documents issued on the Internet site of Kamu SM as necessary; responsible for improving the procedures described in the certificate administration procedures.

Certificate Creation Team Leader: Performs all the operations about planning and realizing the certificate creation, and the delivery of the certificates, coordinates the certificate creation operator.

Certificate Creation Operator: Performs the certificate life cycle operations in accordance with the Certificate Administration Procedures. Controls and archives the incoming and outgoing documents in regard to the certificate life cycle processes.

Certificate Call Support Operator: Answers the phone calls directed to Kamu SM. Informs the certificate owner in accordance with the procedures.

Electronic Certificate Administration Infrastructure (ESYA) and Application Support Manager: Takes the necessary precautions for keeping the ESYA system operational at Kamu SM.

Auditor: An auditor is a person chosen among the units performing compatibility audits in TUBITAK BİLGEM or among Kamu SM's personnel, and responsible for setting up the system audit profile, managing and evaluating the audits, controlling the technical and managerial operations of the system, and preparing reports.

5.2.2. Number of Persons Necessary for Each Operation

Kamu SM ensures the availability of more than one person at the same time for the creation and the revocation processes of certificates belonging to Roots and Sub roots.

Kamu SM ensures the availability of more than one person at the same time for backing up the signature creation data of Root and Sub roots in a separate cryptographic module.

5.2.3. Authentication and Authorization

At every stage of the Kamu SM operations, the authentication and authorization processes are carried out for the persons performing the operations. Therefore only the authorized personnel can access each of the system units. Access to some of the units in the system is made possible 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.

Authentication within the Kamu SM systems is performed by utilizing secure hardware tools, passwords, secret questions and biometric data, and with up-to-date cryptographic methods.

5.2.4. Roles that Require Separation of Duties

One person may be responsible for multiple roles with the exception of the certificate operators.

5.3. Personnel Controls

5.3.1. Personal Background, Experience and Skill Requirements

The personnel are chosen among the persons who can meet the operational and security requirements of the system with their skills, knowledge and experience. The personnel that Kamu SM employs are qualified persons that impose the knowledge and experience about system security, database management, electronic signature technologies and applications, and certificate management.

5.3.2. Background Investigation

The personnel should poses the reliability that the security requirements of Kamu SM administration. The reliability of the personnel is determined by performing a personal history investigation. During the investigation stage before the employment, whether or not the person has been convicted for a reason is investigated.

5.3.3. Training Requirements

The employees are given the necessary education before actively starting their jobs in Kamu SM. Within the education program, the security criteria applied at Kamu SM, the technical and administrative operation of the system, the processes relating their responsibilities, and their duties and responsibilities are explained to the employees.

5.3.4. Requirements and Frequency of Continuous Training

The education programs for the personnel in regard to the changes to Kamu SM systems are repeated as necessary. Basic training is granted to those, who lately started the job.

5.3.5. Frequency and Order of Reassignment

Has not been deemed necessary to regulate.

5.3.6. Punishment of Unauthorized Activities

Related regulations will be applied in the events that Kamu SM personnel creates electronic certificate partially or in full, copies or damages the valid electronic certificates, creates electronic certificate without authorization or utilizes the electronic certificates in purpose, and for other unauthorized activities.

5.3.7. Requirements for Contracted Personnel

In the event that Kamu SM has to work with persons other than its own employees, it performs all the security controls to these persons.

5.3.8. Provided Documentation

The guides and support documents are provided to the employees in accordance with their duties and processes.

5.4. Audit Logs

The activities about key and certificate administration, created during Kamu SM operations, and other activities regarding the system security are logged. Some of the logs are on electronic media, while the others are on paper. These logs may be examined by the auditors during the audits if necessary.

5.4.1. Logged Activities

The following activities performed in the system of Kamu SM are logged on the electronic media or paper:

- Life cycle administration activities of Kamu SM keys
  - Key creation
  - Key backups
  - Key termination
  - Cryptographic module life cycle activities
- Creation and revocation requests for certificates
  - Information about the documents provided by the applicant
  - ID documents provided during the application
  - Electronic or paper forms or documents submitted during the application
  - Information of where the copies of printed documents
  - All valid and invalid application information
- Certificate life cycle administration activities
  - Certificate creation
  - Certificate revocation
  - Issuing CRL
- Other security-related operations
  - All successful or unsuccessful access attempts to the system
  - Security system processes performed by the employees
  - Read, write and modify process performed on the sensitive files, which should be kept safe
  - Changes in the security profiles
  - System crash, hardware errors and other failures
  - Firewall and router operations
  - Visitors' access to Kamu SM

The logs include the time stamp and the user name.

5.4.2. Log Inspection Frequency

The logs relating the system operation are examined in regular intervals. The inspections are made on weekly basis and possible occurrence of a security breach is searched. In addition to that, the logs are examined when unusual operations in the system are detected or in the state of alert. The operations performed upon the investigation are also documented.

The information stored on electronic media or paper that are provided by the certificate owners during the application for a certificate may be examined as necessary or due to legal actions, within the life cycle of the certificate.

5.4.3. Retention Period of Logs

The logs are kept within the system at least for 2 (two) months after the examination. The logs are then archived.

5.4.4. Protection of Logs

The following precautions have been taken for keeping the logs of Kamu SM physically and electronically secure:

- The logs are created by the authorized personnel.
- Unauthorized personnel cannot access the systems where the electronic logs are stored.
- The paper logs are stored in locked rooms and can be accessed only by the authorized personnel.
- The logs cannot be modified, and all necessary security precautions are taken to ensure that.
- The logs that are critical for the system operation and are stored electronically, may be electronically signed by the operating personnel as necessary and saved. This way, any changes in the critical logs can be detected by the system.
- The critical information can be encrypted by KamuSM's keys if necessary.

5.4.5. Backing up Logs

Considering the importance of the system, an online backup of the necessary logs is taken regularly on daily basis when the system traffic is relatively low. A tape library to fulfill the backup requirements and a backup management software to automate the backup process are utilized.

5.4.6. Gathering Logs

The logs are gathered automatically at the levels of application, network and OS. Kamu SM personnel prepare logs during data input regarding the certificate operations.

5.4.7. Notifying the Party Causing the Log

Kamu SM certificate administration system user that initiates the process that causes the log will be notified about the log by the system.

5.4.8. Evaluation of Vulnerability

The technical security controls stated in Chapters 6.5, 6.6 and 6.7 are applied for the systems where the inspection logs are saved.

5.5. Log Archiving

5.5.1. Types of Archived Logs

The following documents, stored electronically or on paper, regarding the certificate application and the life cycle of the certificate are archived in addition to the logs mentioned in Chapter 5.4.1:

- All information and documents provided at the time of application by the certificate owner or the related organization

- Electronic or paper forms submitted during the applications for the creation and revocation of the certificates
- Important correspondences regarding the certificate processes
- All the generated certificates
- All the expired KamuSM Root and sub root certificates
- All the certificate revocation status records issued
- Certificate Policy document
- Certificate Practice Statement document
- Certificate administration procedures
- Certificate Owner Commitment Letters

5.5.2. Retention Period of Archive

The archived information and the documents are stored for at least 7 (seven) years.

5.5.3. Protection of Archive

The archived information and documents are kept electronically and physically safe from unauthorized monitoring, modifications and deletion. Archives cannot be accessed by unauthorized personnel. The environment that archives are retained is chosen in a manner to prevent from damage through the period stated in 5.5.2.

5.5.4. Archive Backup Procedures

The electronic archives that contain critical information are backed up in accordance with Kamu SM Process Continuity Policy.

5.5.5. Time Stamp Requirements of Logs

KamuSM adds time stamps on necessary logs.

5.5.6. Archive Collection System

The archives are gathered electronically or on paper.

5.5.7. Method of Gathering and Authenticating the Archive Information

The archived information is obtained from the authorized personnel. In the event that more than one archived about the same data exist, the archives are compared to ensure the accuracy.

5.6. Key Changeover

The keys and certificates of Kamu SM might be renewed due to expiration or security reasons. Before the expiration of the certificate belonging to Kamu SM, the exchange procedures from the old key pair to the new key pair are performed. The key exchange procedures require the followings:

- The process is initialized minimum 3 (three) years before expiration of the certificate. Issuing certificates with the old keys are avoided.
- Kamu SM keeps publishing the old Kamu SM certificate in order for authentication of the certificates signed by the old signature creation data.

- If the CRL file is signed by the same Kamu SM signature creation data, Kamu SM continues to sign CRL's with the old signature creation data until the certificates created using the old signature creation data expire. The CRL file created for the recently created certificates are signed with the new Kamu SM signature creation data.
- Kamu SM announces the renewal of the keys on http://www.kamusm.gov.tr and notifies the organizations it provides the certificate service.

5.7. Things to Do on Loss of Reliability and Failures

5.7.1. Correcting Loss of Reliability

In cases of losing reliability, the determined processes for providing the safe operation of the certificate administration system as soon as possible, notifying the related parties, and minimizing the negative impacts will be operated.

5.7.2. Hardware, Software or Data Corruption

The cases of hardware failures, software failures or data corruption are reported and necessary process to fix the failure/error are initiated.

In order for maintaining the continuity of the process, the active devices and storage space network components operate with backup units. The storage unit is capable of making data synchronization with a data storage unit located at a different physical location. The troubleshooting process includes the evaluation of the cause of the failure, fixing the failure and moving the Kamu SM services to safe backup environment if necessary.

The processes to be operated during a theft may be applied if necessary and the system is taken back online.

5.7.3. Losing the Confidentiality of Signature Creation Data

In case of a suspicion about the confidentiality of the signature creation data used by Kamu SM in signing certificates, or in case of detecting such a situation, the related certificate is revoked as soon as possible, and the following processes are performed:

- Kamu SM announces the revocation of its certificate, along with the revocation reason at http://www.kamusm.gov.tr and notifies the related organizations in writing.
- Kamu SM makes an explanation about how the certificate owners will be affected from the situation, and warns the users for not trusting the certificates created with the old private key.
- Kamu SM states the revocation of its certificate in the CRL file it issues.
- A necessary part or all of the SSL certificates created by Kamu SM are revoked. The notification about the revocation is submitted to the certificate owners and the related organizations in the shortest time.
- Kamu SM stops responding the requests for certificates.
- Related parties are continuously informed of the current situation of Kamu SM.
- Kamu SM carries out the signature creation data termination process.
- Kamu SM creates a new key pair set and certificate, and informs the parties of the new certificate.

- With the renewal of Kamu SM key pair set, the process of updating the revoked certificates as per the users' request begins.

5.7.4. Re-operation after Failure

Kamu SM defines the methods and processes necessary for ensuring the safe re-operation of the system after a failure or disaster under Kamu SM Work Continuity Plan.

Kamu SM continuously evaluates and tests the Kamu SM Work Continuity Plan that will provide the re-operability after failure.

5.8. Terminating Certificate Services

When Kamu SM may stop its operation in any accordance, performs the following operations in such cases:

- Notifies the organizations it provides the certificate services in writing, and the certificate owners by email, 3 (three) months prior to the date of stopping the certificate services.
- Announces the information about ending services to public over the internet and on the top 3 (three) national newspapers with the largest circulation.
- Does not accept applications for certificates and will not create new certificates after announcement.
- Revokes the SSL certificates, informs the third parties about the revocation via CRL and OCSP. Notifies the organizations in writing, and certificate owners by email about the information on the revoked certificates.
- Continues to issue the certificates on the latest CRL file until the revoked certificates expire.
- Continues to issue the certificate about the signature creation data that is used to sign the CRL file until the CRL file expires.
- Terminates the signature creation data used for signing the certificates.
- Keeps all related records and archives for 7 (seven) years accordingly.

6. Technical Security Controls

The systems that are used for generating the key pairs and access data for Kamu SM itself and the certificate owners, and where the certificate administration processes carried out, complies with CWA 14167-1 and ETSI TS 101 456.

6.1. Key Pair Creation and Installation

6.1.1. Key Pair Generation

6.1.1.1. Root and Sub root Key Pair Generation

The key pairs for Roots and Sub roots are generated using a secure software an/or hardware tested for safe key generation, on systems that are not connected to any network, under supervision of more than one educated personnel, and in a room where unauthorized personnel cannot access. The created signature creation data is stored in a safe cryptographic module. The module is not taken out of the room. All activities are recorded and approved by the personnel performing the operation.

The cryptographic module in which the signature creation data is stored complies with the standards stated in Chapter 6.2.1.

6.1.1.2. Key Pair Creation for Certificate Owner

Key pair generation for the SSL certificates is executed by the certificate owner.

6.1.2. Delivery of Signature Creation Data to Certificate Owner

Has not been deemed necessary to regulate.

6.1.3. Delivery of Signature Verification Data to CA

The SSL certificates applicants deliver the authentication data to Kamu SM in PKCS#10 format as a request for certificate signing via corporate e-mail address, after their respective applications are accepted.

6.1.4. Providing Access to Certificates of CA

The Root CA and sub root certificates of Kamu SM can be accessed over the Internet. The certificate storage environment is protected against unauthorized editing and deletion.

Certificates belonging to Kamu SM are issued via the web page of Kamu SM.

The hash value and hash algorithm of the root and sub root certificates are issued at the web address http://depo.kamusm.gov.tr and announced to public via the top 3 (three) national newspapers with the largest circulation in 7 (seven) days following Kamu SM's becoming operational.

6.1.5. Key Sizes

The size of RSA public key algorithm signature key pair set of Kamu SM roots and sub roots are minimum 2048 bits.

The size of RSA signature key pairs used for signing the revocation status records announced via OCSP Responder are minimum 2048 bits.

The size of RSA key pairs that belong to the certificate owners of the SSL certificates created by Kamu SM are minimum 2048 bits.

6.1.6. Key Generation Parameters and Quality Checking

The security of the algorithms used in the key generation by Kamu SM has been proved and accepted worldwide. The methods utilized in algorithm realization comply with the necessary security criteria. The key generation hardware and software are passed from the necessary security tests.

6.1.7. Key Usage Purposes

It is stated in the "Key Usage" and the "Extended Key Usage" extension thereof on the certificate corresponding to the relevant signature creation data, for which purposes such signature creation data generated by Kamu SM may be used.

6.2. Protecting Signature Creation Data

6.2.1. Cryptographic Module Standards

The signature creation data of KamuSM is created using secure hardware and/or software, stored in a secure cryptographic module and does not get out of this module as long as it is valid.

The cryptographic module possesses the following security functions:

- Ensures the confidentiality and integrity of the signature creation data until expiration.
- Performs the authorization and authentication processes during the access to the module.
- The access permission can be defined to be controlled by more than one person.
- Limits the access to the services in accordance with the roles assigned to the users.
- The proper functionality can be testes, switches to safe mode if an error occurs during testing.
- All possible physical precautions against the activities that may cause damage such as unauthorized access and utilization of the module.
- The module deletes the data it stores in case of an unauthorized access attempt.
- Enables the safe back up of the signature creation data.

The cryptographic module complies with at least one of the following security standards:

- Level 3 or more, according to FIPS PUB 140-1 or FIPS PUB 140-2

6.2.2. Access to Signature Creation Data under Control of Multiple Persons

The access to the room where the signature creation data of Kamu SM is stored, is provided by at least 2 (two) employees.

6.2.3. Regaining Signature Creation Data

Has not been deemed necessary to regulate.

6.2.4. Backing up Signature Creation Data

The backup process of the signature creation data of Kamu SM is performed by more than one authorized personnel. The security precautions for the backup procedure are the

same with the precautions taken for the signature creation data. The backed up signature creation data is stored in a physically and electronically secure cryptographic hardware device, which is kept away from the access of unauthorized persons. The secure hardware device is kept within an environment with the same security conditions as the environment where the real signature creation data is stored.

The signature creation data of the certificate owners are not present at Kamu SM.

6.2.5. Archiving Signature Creation Data

The signature creation data that belong to Kamu SM and the certificate owners are not archived.

6.2.6. Signature Creation Data Transfer Into or From a Cryptographic Module

The signature creation data of Kamu SM is saved on the cryptographic module upon creation. The operation is performed with reliable methods and under supervision of more than one authorized personnel.

6.2.7. Storing Signature Creation Data on Cryptographic Module

Signature creation data that belong to Kamu SM are stored in physically and electronically secure cryptographic hardware devices where unauthorized persons cannot access. Taking the signature creation data out of the device is avoided, except for back up purposes. The signature creation data are kept cryptically in a safe cryptographic module with safe algorithms and method.

6.2.8. Access to Signature Creation Data

Access to the signature creation data of Kamu SM is under the joint supervision of multiple personnel. In order to access to the room where the signature creation data is stored, all authorized personnel should be ready at the same time and they must pass the authentication and authorization tests. In the event that sufficient number of authorized personnel is not ready or the authentication fails, access to the room where the signature creation data is stored, is blocked.

The signature creation data is closed to access when encrypted in the cryptographic module. The data allowing the access must be provided in order to open access. Allowing the access of the signature creation data and bringing it into use is under the joint supervision of multiple personnel.

6.2.9. Blocking Access to Signature Creation Data

The access to the signature creation data of Kamu SM is automatically cut off once session is closed after the utilization for signing process, and stored encrypted until next utilization. In order for providing access again, the procedures stated in Chapter 6.2.8 must be processed once again.

6.2.10. Deleting Signature Creation Data

After the usage periods of the signature creation data of Kamu SM expire, the original and all backups are irreversibly deleted from the environment with suitable methods. To perform the deletion process for the signature creation data of Kamu SM, sufficient number of authorized personnel must be ready in accordance with Chapter 6.2.8.

6.2.11. Evaluation of Cryptographic Module

Kamu SM uses cryptographic modules that comply with the standards specified in 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Archiving Signature Verification Data

The signature verification data that belong to Kamu SM and the certificate owner are saved in the certificates and archived for 7 (seven) years after the expiration of the certificates. The archives of the certificates are placed in the locations where necessary precautions against corruption and deletion by unauthorized persons are taken.

6.3.2. Usage Periods of Certificate and Signature Creation and Verification Data

The utilization period of the signature creation data is equal to the utilization period of the certificate defined in the certificate. The utilization of the signature creation data ends upon the expiration or revocation of the certificate. However, the signature verification data is used for authenticating old signatures even if the certificate expires.

The utilization periods of the key pairs that belong to Kamu SM and the certificate owner are determined in accordance with the key length and signature algorithm used. 2048-bit RSA key pairs of Kamu SM are used for maximum 10 (ten) years.

The expiration date of the created certificates may not exceed the expiration date of the root and sub root certificates of Kamu SM.

6.4. Activation Data

The access control data of KamuSM personnel include the access passwords, other data within the safe hardware tools regarding access control, and biometric data.

6.4.1. Generation of Activation Data

The access control data used in Kamu SM systems are generated in the physically and electronically secure environments that cannot be accessed by unauthorized persons.

6.4.2. Protection of Activation Data

The access control data utilized in Kamu SM system are known only by the authorized personnel.

6.4.3. Other Aspects of Activation Data

Has not been deemed necessary to regulate.

6.5. Computer Security Controls

6.5.1. Technical Requirements Concerning Computer Security

Necessary precautions against malware are taken in Kamu SM's systems. The system occupies an intrusion detection system that includes network-based and server-based sensors. Antivirus clients are installed on all servers which can be managed by the central administration unit. The systems that are used for critical operations are kept offline. Necessary security is provided for ensuring the protection of the information against corruption and leaks, and maintain the continuity of the operations. Copies of all the installed

software are taken and the improvement activities about the system security are applied immediately.

6.5.2. Security Level Provided by the Computer System

Has not been deemed necessary to regulate.

6.6. Life Cycle Technical Controls

6.6.1. System Improvement Controls

The main controls performed during the system development are stated below:

- Necessary quality and security precautions are taken.
- Personnel complying with the defined security criteria are employed.
- Backup copies of all installed software are taken.
- Backups of the components that keep the system information are taken in order for maintaining the continuity of the certificate processes.
- Necessary security precautions are taken while connecting the system to web.
- Before using third party software during the setup, the system is secured against viruses and unofficial software are prevented from entering into the system. All security precautions are applied on this subject, and all improvement actions are performed immediately.
- The system status is monitored closely at the early stages of the system in order for detecting abnormal activities.
- Authentication of the information such as identity and passwords are performed for providing access to the developing system.
- The controls performed during the system development comply with TS ISO/IEC 27001 requirements.

6.6.2. Security Management Controls

Security management audits are performed at least once every year in order to prove the secure operation of the software and hardware products installed on the system, and network, as planned. Insecure activities and authorizations within Kamu SM are announced and corrective actions are taken.

6.6.3. Life Cycle Security Controls

Has not been deemed necessary to regulate.

6.7. Network Security Controls

Necessary network security audits are conducted in accordance with the latest technological improvements. The system utilizes firewalls when connecting the open extranet. Network and system administration servers are used for monitoring the status and performances of the servers and active devices, obtain performance reports based on the past and predict the performance trends for the future.

Network and system management agents are installed on the servers. The management software gathers the disk, memory and processor usage data from these agents and shows these information in real time. The thresholds are determined for the resources important for the system operation and the system manager is automatically modified on exceeding these thresholds. Network and system management software keeps the gathered software in a central database. This allows querying of the data at anytime and generating retrospective reports.

Separate networks are set up for the systems utilized for performing high security operations. The systems used for critical operations are not connected to a network.

6.8. Time Stamping

Has not been deemed necessary to regulate.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profiles

In this chapter, the contents of Root, Sub root, SSL and S/MIME certificates generated by Kamu SM are explained.

7.1.1. Version Number

Kamu SM supports the "ITU-T X.509 V.3" certificate standard.

7.1.2. Certificate Extensions

The certificates distributed by KamuSM include required fields such as the serial number of the certificate defined in x.509 V.3 format, the validity date, related signature verification data, the names of the certificate owner and Kamu SM, and the electronic signature of Kamu SM, as well as X.509 V.3 certificate extensions. The certificate extensions included in the certificate are determined based on the requirements of the application where the certificate will be used.

The contents of Root, Sub root ve SSL certificates generated by Kamu SM are available in Appendix-A.

Some of the extensions are defined as critical. The certificate should not be used unless the critical extensions are identified by the application.

7.1.3. Algorithm Object Identifiers

Specified in Appendix-A.

7.1.4. Name Forms

The name space within the certificates created by Kamu SM complies with "ITU X.500 Distinguished Name" format.

7.1.5. Name Constraints

Specified in Chapter 3.1.

7.1.6. Certificate Policy Object Identifier

Within the content of every certificate generated by Kamu SM, the object identifier belonging to the related certificate policy has been given in order to specify as per which certificate policy, such certificate shall be used. For SSL certificates, object identifying number {2.16.792.1.2.1.1.5.7.1.2} belonging to this document is used.

7.1.7. Usage of Policy Constraints Extension

Has not been deemed necessary to regulate.

7.1.8. Policy Qualifiers

"Certificate Policy Extension" implies that the principles and basics complied with during the creation and management of the certificates are Kamu SM CP and Kamu SM CPS. The certificate policy object identifiers of CP/CPS document, which show the rules followed during the creation and management of the SSL certificates, are placed in the "Certificate Policy Extension" of the SSL certificate created by Kamu SM. The internet address where the

Kamu SM CP/CPS document is stored, is written as "Policy Qualifier" within "Certificate Policy Extension".

Third parties take actions using the certificates in accordance with the policies and practice statement defined in CP/CPS upon checking the "Certificate Policy Extension".

Within the content of "Certificate Principles Extension" on the SSL certificates generated by Kamu SM, {2.16.792.1.2.1.1.5.7.1.2} lies as the object identifying number and http://depo.kamusm.gov.tr/ilke stands as the principle qualifier.

7.1.9. Processing of Critically Specified Certificate Policies Extension

Has not been deemed necessary to regulate.

7.2. CRL Profile

7.2.1. Version Number

CRL's created by Kamu SM comply with "ITU X.509 V.2" CRL format.

7.2.2. CRL and CRL Entry Extensions

The created CRL's include the following information in accordance with "ITU X.509 V.2" CRL format:

- Name information about Kamu SM that creates CRL
- Object identification numbers of the algorithms used to sign CRL (Kamu SM uses SHA-256 hash algorithm and RSA open key signing algorithm to sign the CRL it issues).
- Issue date of CRL
- CRL number
- Next issue date of CRL
- The following information about the revoked certificates:
    - Serial number of the certificate
    - Revocation date of the certificate
    - Revocation reason of certificate
- The electronic signature created by Kamu SM
- "Key Identifier" number of Kamu SM's certificate used to authenticate the signature of CRL

7.3. OCSP Profile

7.3.1. Version Number

Online Certificate Status Protocol supports RFC 2560 V.1.

7.3.2. OCSP Extensions

OCSP queries should include the following information.

- Protocol version
- Target certificate identifier (hash algorithm used, DN hash of certificate provider CA, signature verification data hash of certificate provider CA, serial number of certificate)

OCSP responses should include the following information.

- Version information
- Name of responder
- Respond name for each certificate (certificate identifier (serial number of certificate), certificate status, respond validity period)
- OID of the signature algorithm used
- OCSP responder's signature

All valid OCSP answers are signed by OCSP responder. The error messages of invalid OCSP queries are not signed.

Online Certificate Status Protocol supports the "OCSP" format expressed in RFC 2560. The responds received from OCSP Responder are evaluated as follows:

Good : The certificate is valid.

Bad : The certificate is suspended, revoked, or not yet activated.

Unknown : No information found for the certificate in question.

The extensions stated in RFC 2560 cannot be used in OCSP respond format.

8. Compliance Audits

In this Chapter, performing audits on the compliance of Kamu SM certificate management system with CP/CPS document are explained.

8.1. Frequency of Compliance Audit

The compliance of Kamu SM certificate management system with the conditions stated in this CP/CPS document is controlled at least once every years. The audits are performed by personnel authorized by Kamu SM.

8.2. Qualifications of Auditor

The auditor should possess a good understanding on the subjects mentioned in CP/CPS document, have knowledge on open key infrastructures, and should be experienced in compliance audits.

8.3. Auditor's Relationship with Auditee

The auditor is chosen among the persons performing compatibility audits in TÜBİTAK BİLGEM or among Kamu SM's personnel.

8.4. Scope of Audit

The compliance of the certificate management procedures that explains the certificate management processes in detail, and the security and operational processes of Kamu SM's internal operations with CP/CPS document is controlled.

8.5. Things to Do on Inadequacy Detection

In case of detecting that Kamu SM does not fulfill the requirements of CP/CPS documents, the auditor informs the related persons about the inadequate stages in the processes with a report. The corrective actions are determined with the lead of Kamu SM management, and the actions are performed.

In case of detecting that the requirements of CP/CPS documents have not been satisfied during the system setup, operation or maintenance stages, the following actions are taken:

- The auditor notes the inadequate stages of the processes and notifies the related parties in 2 (two) days.
- Kamu SM corrects the inadequacies detected in accordance with the practice statements defined in CP/CPS document.
- In case of detecting an inadequacy in the critical operations about the certificate management, Kamu SM stops the related operations until the corrections are made.

In addition, related regulations will be applied in case that Kamu SM personnel creates electronic certificate partially or in full, copies or damages the valid electronic certificates, creates electronic certificate without authorization or utilizes the electronic certificates in purpose, and for other unauthorized activities.

8.6. Reporting the Results

The audit results are notified to Kamu SM management as a report. Kamu SM management ensures the correction of the conditions stated in the report that do not comply with CP/CPS as soon as possible.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Creation and Renewal Fees

The organizations or certificate owners are charged for the created certificates. The pricing and the payment method are mentioned on the offers sent by Kamu SM or at Kamu SM's website.

Kamu SM will not request any payments if the certificates are revoked or updated due to reasons out of certificate owner's control, such as theft or loss of Kamu SM's signature creation data, loss of reliability or confidentiality of the data, changes in the certificate policies or creation of faulty certificates.

9.1.2. Certificate Access Fees

Kamu SM issues the certificates that belong to itself free of charge.

9.1.3. Access Fees to Revocation Status Record

Kamu SM does not charge the certificate owner or third parties for announcing the revocation status record via CRL or OCSP.

9.1.4. Fees for Other Services

The operations performed on the electronic environment or over the call center in accordance with the certificate management procedures are not charged.

Kamu SM does not charge the certificate owner or third parties for providing access to the information or documents issued from its repository.

9.1.5. Refunds

If the certificate owner figures out that he cannot use his certificate during the initial controls after receiving the certificate, and if the problem is arising from a mistake that Kamu SM has made, the price paid for the certificate will be refunded as per the certificate owner's request.

9.2. Financial Liability

9.2.1. Insurance Coverage

Kamu SM is operated by Informatics and Information Security Research Center within the body of TÜBİTAK (The Scientific and Technological Research Council of Turkey). TÜBİTAK – BİLGEM does not apply any insurance for the moment regarding the SSL certificates addressed to certificate owners and to the third parties using the certificate.

9.2.2. Other Assets

Has not been deemed necessary to regulate.

9.2.3. Certificate Financial Liability Insurance

Has not been deemed necessary to regulate.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The business plans, sales data, commercial secrets and information provided in the confidential agreements, shared by Kamu SM and the parties it provides services, are considered commercial information. Unless otherwise stated, all documents are also considered confidential.

9.3.2. Information that is not Confidential

All kinds of documents issued on http://depo.kamusm.gov.tr/ilke by Kamu SM and the information in the certificates are not considered as confidential.

9.3.3. Responsibility to Protect Confidential Information

Kamu SM and related parties will not share the commercial information mutually with third parties. They take the necessary precautions in this purpose.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Has not been deemed necessary to regulate.

9.4.2. Information Considered as Private

Personal informations include the information provided by certificate owner to Kamu SM, such as contact information such as addresses and phone numbers, which are to be used in the authentication, authorization and certificate management procedures.

9.4.3. Information that is not Considered as Private

The information in the certificates generated by Kamu SM is not considered as confidential unless otherwise stated in the commitment letters/contracts between the parties.

9.4.4. Responsibility To Protect Confidential Information

Kamu SM does not request information from the applicant, except for the information necessary for providing a certificate. Kamu SM does not use the gathered personal information for purposes other than providing certificate services, does not share with third parties, does not keep these information in public domains without the permission of the certificate owner.

Kamu SM takes necessary precautions for ensuring the privacy and blocking the access to and unauthorized use of the information requested during the application and within the life cycle of the certificate. Only the authorized personnel can access the personal information of the certificate owners.

9.4.5. Permission to Use Confidential Information

Kamu SM may share the personal information with third parties with the written permission of the certificate owner.

9.4.6. Exposing Information due to Court Order

The personal information of the Kamu SM certificate owners may be exposed in case of a court order.

9.4.7. Other Headings

Has not been deemed necessary to regulate.

9.5. Intellectual Property Rights

The intellectual property rights for all the certificates and documents created by Kamu SM, and the information developed based on this CP/CPS document belong to Kamu SM.

9.6. Representations and Warranties

Kamu SM, certificate owners, government institutions and organizations that certificate owners are linked to and third parties fulfill the liabilities mentioned in certificate contracts and commitment letters.

The responsibilities of the system components in order to ensure the safe operation of KamuSM as a CA are mentioned below.

9.6.1. CA Representations and Warranties

Kamu SM's responsibilities as a CA are as follows:

- Employing qualified personnel in accordance with the requirements of the service,
- Providing the certificate operations in regard to the policies and fundamentals stated,
- Issuing CP and CPS documents on the repository accessible by anyone,
- Creating key pairs for Roots and sub roots, and creating certificates for these key pairs,
- To publish the root and root certificates in such medias accessible by end users,
- Proving the identities of the real and legal persons it provides the certificates based on official documents reliably,
- Accepting the applications for SSL certificates accordingly and authenticating the applicants by performing necessary controls over the documents and application forms of the applicants,
- Ensuring the accuracy of the information within the certificate based on submitted documents,
- Not providing certificates to persons that do not meet the necessary application conditions,
- Notifying the related persons about the application results after evaluating the certificate applications,
- To generate certificates for those, whose certificate appeals are accepted,
- To issue the certificates of the respective owners in such medias accessible by end users, unless otherwise mentioned in the application form and the contracts between parties,
- Accepting the certificate renewal/update applications as specified in CP/CPS, and performing the necessary renewal/update operations,
- Accepting the certificate revocation applications as specified in CP/CPS, and performing the necessary revocation operations on time,

- To revoke the related certificate in case any certificate usage non-complying with the issued CP/CPS document and SSL Commitment Letter is detected,
- Issuing the revoked certificate information in the certificate revocation lists, or announcing via OCSP responder,
- Taking every precaution to ensure the integrity and accessibility of the certificates and revocation status records,
- Taking necessary precautions for protecting the information of the certificate owners stored electronically or on paper, not sharing these information with third parties unless asked by a court order,
- Logging all activities regarding certificate creation, management and revocation,
- Safekeeping all paper and electronic logs created during the processes in accordance with periods stated in CP/CPS,
- Issuing the hash value of the root CA at Kamu SM's Internet site, announcing to public via top 3 (three) national newspapers with highest circulations and submitting a copy of the newspaper announcements to Telecommunication Institution.

9.6.2. RA Representations and Warranties

Has not been deemed necessary to regulate.

9.6.3. Subscriber Representations and Warranties

The responsibilities of the certificate owner are as follows:

- To perform the transactions of certificate application, revocation and others as described in the related CP/CPS document and in accordance with the methods specified in Kamu SM certificate management procedures,
- Declaring accurate information during the certificate application, renewal, update and revocation activities,
- To check the accuracy of the information on the personally issued certificate,
- Ensuring the security of the signature creation data,Applying Kamu SM in the shortest possible time for revoking the certificate, in case of having any suspicions on the confidentiality of the signature creation data,
- To appeal to Kamu SM for the immediate revocation of the certificate, in case the information stored within the certificate content generated for itself by Kamu SM has been changed,
- Informing Kamu SM immediately of any changes in the information declared during the application for or validity period of the certificate,
- Not using the revoked or expired certificates,
- Not utilizing the signature creation date for signing SHS certificate,
- To use the provided certificate in accordance with CP/CPS documents, within the terms mentioned in the SSL Commitment Letter.

TÜBİTAK BİLGEM reserves the right to recourse the indemnities it pays to third parties due to the violation of the above mentioned Responsibilities, to the related certificate owners.

9.6.4. Relying Parties Representations and Warranties

Before proceeding with any activities regarding the certificates, third parties are responsible for making the following validity controls:

- Verifying that the certificates are being utilized in regard to their purpose,
- Checking whether the certificate has expired or not,
- Checking the validity of the certificate via CRL or OCSP Responder,
- Authenticating the integrity of the revocation status record gained from CRL or OCSP Responder with the signature verification data stored in the related certificate,
- Authenticating the certificate by using the signature verification data stored in the Kamu SM Sub root certificate,
- Authenticating the Kamu SM sub root certificate by using the signature verification data stored in the root certificate,
- Authenticating the Kamu SM root certificate by checking the certificate hash value,
- Validating that the certificate has the signature creation value that corresponds the signature verification data.

9.6.5. Representations and Warranties of Other Parties

Has not been deemed necessary to regulate.

9.7. Disclaimer

The responsibilities between Kamu SM and the organizations or institutions of the certificate owners are terminated in accordance with the SSL Commitment Letter.

9.8. Limitations of Liability

The limitations regarding the liabilities of Kamu SM and parties that receive certificate services are also specified in SSL Commitment Letter.

9.9. Indemnities

The damages arising from not fulfilling the responsibilities by Kamu SM and parties that get the certificate service are dissoluted with reserving the rights and assets realized until that time.

9.10. Agreement Duration and Termination of Agreement

The certificate owners cooperate with Kamu SM in accordance with SSL Commitment Letter.

The organizations and the certificate owners agree to fulfill the conditions stated in CP/CPS documents as well as the conditions stated in the certificate management procedures during the certificate services.

As long as Kamu SM provides certificate service, it fulfills the conditions in CP/CPS document, certificate management procedures, SSL Commitment Letter delivered to certificate owner.

9.10.1. Agreement Duration

The durations of the SSL Commitment Letter signed by the certificate owner are equal to the validity period of the certificate. However, if the certificate is revoked, the validity of the commitment letter also expires.

9.10.2. Termination of Agreement

The SSL Commitment Letter signed by the organization can be terminated if following conditions occur:

- In case of the termination request of one party in accordance with the agreement
- Expiration of the agreement
- Termination of the contract with the mutual agreement of both parties
- Violation of the agreement by one of the parties: In case that one party fails to fulfill its responsibilities in accordance with the contract, the other party allows the violating party 5 (five) days to make up for its responsibilities. If the violation is not eliminated, or reserving the right for claim for indemnities and losses, the responsibilities in question are not fulfilled, the agreement can be unilaterally terminated.
- Kamu SM may revoke the certificates of the certificate owners and terminate SSL Supply Agreement in the event of a security breach as stated in Chapter 5.7.3.
- Kamu SM may revoke the certificates of the certificate owners and terminate SSL Supply Agreement if Kamu SM ends the certificate services as stated in Chapter 5.8.

The Kamu SM Letter of Commitment, Certificate Owner Letter of Commitment or the Certificate Contract may be terminated upon the following conditions:

- Revocation of certificate by certificate owner
- Expiration of certificate
- Revocation of the certificate of the certificate owner by Kamu SM due to certificate owner's violations of Certificate Contract or Certificate Owner Commitment Letter
- Revocation of the certificate of the certificate owner by Kamu SM due to occurrence of a security breach as mentioned in Chapter 5.7.3
- Revocation of the certificate of the certificate owner by Kamu SM if Kamu SM ends the certificate services as stated in Chapter 5.8.

9.10.3. Effects of Termination of Agreement

With the termination of SSL Supply Agreement, the responsibilities of the organization acquiring the service for following the conditions in accordance with the agreement and CP/CPS document are terminated. Kamu SM stops accepting certificate applications from the organization. However, previous applications may proceed in accordance with the reason for termination of the agreement and as per the organization's request.

With the termination of Certificate Contract or Certificate Owner Commitment Letter, the responsibilities of the certificate owner in accordance with the commitment letter and CP/CPS document are also terminated. Kamu SM shall not be held responsible for the losses of the certificate owner due to violation of the commitment letter by the certificate owner.

Even though the agreement and commitments are terminated, Kamu SM continues to fulfill its responsibilities about the distributed certificates. Kamu SM continues to provide services of allowing access of the parties to the distributed certificates and to the revocation status records, as well as storing the archives and logs mentioned in 5.4 and 5.5.

9.11. Communication with Participants and Personnel Notification

Kamu SM informs the certificate owner and/or the related organization about the results of the certificate applications, and revocation, renewal or update requests in accordance with the certificate management procedures. Notifications are made via phone, fax or emails. In case of changes in the email address of the certificate owner provided on the application form, the new email address is considered as valid address for formal notifications.

The notifications regarding the critical activities of certificate management are made via a formal letter.

The conditions and methods of communication between the certificate owner or organizations during the certificate management activities, are stated in details in Kamu SM's certificate management procedures.

9.12. Amendment

9.12.1. Amendment Procedures

This CP/CPS document has been written by Kamu SM. The modifications in this CP/CPS document might be in forms of additions or changes, while Kamu SM might decide to renew the document completely. If any part of this CP/CPS document is found to be wrong or invalid, other parts of Kamu SM Sİ/SUE shall still be valid until the CP/CPS document is updated.

9.12.2. Notification Mechanism and Frequency

The changes in CP/CPS document are announced by issuing the updated document on Kamu SM repository. The updated document is issued in maximum 1 (one) week from the repository and becomes valid on the date of issuing.

9.12.3. Cases that Require Changing OID

Has not been deemed necessary to regulate.

9.13. Dispute Resolution

All disputes between the parties should be resolved with negotiation. For the resolution of disputes, countersigned contracts, letters of commitment, Kamu SM Certificate Policy and Kamu SM CPS documents are referred to. If the conflicts cannot be resolved via negotiation, Republic of Turkey Gebze Law Courts are authorized.

9.14. Applicable Law

Republic of Turkey - Gebze Courts are in charge and authorized for the resolution of such disputes.

9.15. Compliance with Applicable Laws

In the event that the clauses in the CPS/CPS document violate the regulations to be applied in the future, the necessary modifications are made to the document in order to comply with the regulation.

9.16. Other Conditions

Has not been deemed necessary to regulate.

APPENDIX-A Certificate Profiles

a) Root CA: TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3

Version	V3
Serial Number	11
Signature Algorithm	RSA with sha-1 {1 2 840 113549 1 1 5}
Certificate Issuer	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Valid From	24 August 2007 Friday 13:37:07
Valid To	21 August 2017 Monday 13:37:07
Subject	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Subject Public Key	2048 bit RSA {1 2 840 113549 1 1 1}
Extensions	**Value**
Subject Key Identifier	Critical=No; bd 88 87 c9 8f f6 a4 0a 0b aa eb c5 fe 91 23 9d ab 4a 8a 32
Key Usage	**Critical=Yes**; Certificate Signing, Offline CRL Signing, CRL Signing
Basic Constraints	**Critical=Yes**; Subject Type=CA; Path Length Constraint=None

b) Sub CA: TUBITAK Cihaz Sertifikası Hizmet Sağlayıcı - Sürüm 4

Version	V3
Serial Number	00 d4 a3 e1 ca 01 7a
Signature Algorithm	RSA with sha-256 {1 2 840 113549 1 1 11}
Issuer	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Valid From	18 December 2015 Friday 16:01:51
Valid To	21 August 2017 Monday 14:37:07
Subject	CN = Cihaz Sertifikası Hizmet Sağlayıcı - Sürüm 4 OU = Kamu Sertifikasyon Merkezi O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Subject Public Key	2048 bit RSA {1 2 840 113549 1 1 1}
Extensions	**Value**
Authority Key Identifier	Critical=No; bd 88 87 c9 8f f6 a4 0a 0b aa eb c5 fe 91 23 9d ab 4a 8a 32

Subject Key Identifier	Critical=No; 68 42 55 3f c9 00 ff d7 85 62 7d 41 9a bb 86 96 27 57 60 19
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=2.16.792.1.2.1.1.5.7.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.kamusm.gov.tr/BilgiDeposu/KSM_CES_SUE [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
CDP	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.kamusm.gov.tr/BilgiDeposu/KOKSIL.v3.crl
Authority Info Access	[1] Authorized Info Access Access Method=Certificate Authorized Issuer (1.3.6.1.5.5.7.48.2) Other Name: URL= http://www.kamusm.gov.tr/BilgiDeposu/KOKSHS.v3.crt [2] Authorized Info Access Access Method= Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Other Name: URL= http://ocspkok3.kamusm.gov.tr

c) End-Entity SSL Certificate Template

Version	V3
Serial Number	A unique number
Signature Algorithm	RSA with sha-256 {1 2 840 113549 1 1 11}
Issuer	CN = Cihaz Sertifikası Hizmet Sağlayıcı - Sürüm 4 OU = Kamu Sertifikasyon Merkezi O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Valid From	Certificate creation time
Valid To	Certificate expire time
Subject	CN = Web site DNS name OU = Applicant organization department name O = Applicant organization name L = Location of applicant S = Province of applicant C = Country code of applicant (TR)
Subject Public Key	2048 bit RSA {1 2 840 113549 1 1 1}
Extensions	**Value**
Authority Key Identifier	Critical=No; 68 42 55 3f c9 00 ff d7 85 62 7d 41 9a bb 86 96 27 57 60 19
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 Encryption

Basic Constraints	Critical=No; Subject Type=End Entity; Path Length Constraint=None
Certificate Policy	[1] Certificate Policy: Policy Identifier=2.16.792.1.2.1.1.5.7.1.2 [1.1] Policy Qualifier Info: Policy Qualifier Identity=CPS Qualifier= http://depo.kamusm.gov.tr/ilke [1,2] Policy Qualifier Info: Policy Qualifier Identity=User Notice Qualifier= Notice Text= Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
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)
CDP	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://depo.kamusm.gov.tr/ssl/CSHSIL.v4.crl
Authority Info Access	[1] Authorized Info Access Access Method=Certificate Authorized Issuer (1.3.6.1.5.5.7.48.2) Other Name: URL= http://depo.kamusm.gov.tr/ssl/CSHS.v4.cer [2] Authorized Info Access Access Method=Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Other Name: URL=http://ocspces4.kamusm.gov.tr