PUBLIC

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM SSL CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

Document ID
YON.01.07
Version
v.3.11.1
Date
14.10.2026

PUBLIC

Copyright Notice

Copyright Kamu SM 2016. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of Kamu SM. Requests for any other permission to reproduce this Kamu SM document (as well as requests for copies from Kamu SM) must be addressed to:

Kamu Sertifikasyon Merkezi
TÜBİTAK Yerleşkesi, P.K. 74
Gebze 41470 Kocaeli, TURKEY
https://kamusm.bilgem.tubitak.gov.tr

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

TABLE OF CONTENTS

1. INTRODUCTION 10

1.1. OVERVIEW 11
1.2. DOCUMENT NAME AND IDENTIFICATION 11
1.3. PKI PARTICIPANTS 13
1.3.1. Certification Authorities 13
1.3.2. Registration Authorities 14
1.3.3. Subscribers 14
1.3.4. Relying Parties 14
1.3.5. Other Participants 14
1.4. CERTIFICATE USAGE 14
1.4.1. Appropriate Certificate Uses 14
1.4.2. Prohibited Certificate Uses 14
1.5. POLICY ADMINISTRATION 15
1.5.1. Organization Administering the Document 15
1.5.2. Contact Person 15
1.5.3. Person Determining CPS Suitability for the Policy 15
1.5.4. CPS Approval Procedure 15
1.6. DEFINITIONS AND ACRONYMS 15
1.6.1. Definitions 15
1.6.2. Acronyms 18

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 19

2.1. REPOSITORIES 19
2.2. PUBLICATION OF CERTIFICATION INFORMATION 19
2.3. TIME OR FREQUENCY OF PUBLICATION 19
2.4. ACCESS CONTROLS ON REPOSITORIES 20

3. IDENTIFICATION AND AUTHENTICATION 20

3.1. NAMING 20
3.1.1. Types of Names 20
3.1.2. Need for Names to be Meaningful 20
3.1.3. Anonymity or Pseudonymity of Subscribers 20
3.1.4. Rules for Interpreting Various Name Forms 20
3.1.5. Uniqueness of Names 20
3.1.6. Recognition, Authentication, and Role of Trademarks 21
3.2. INITIAL IDENTITY VALIDATION 21
3.2.1. Method to Prove Possession of Private Key 21
3.2.2. Authentication of Organization and Domain Identity 21
3.2.2.1. Identity 22
3.2.2.2. DBA/Tradename 22
3.2.2.3. Verification of Country 22
3.2.2.4. Validation of Domain Authorization or Control 22
3.2.2.5. Authentication for an IP Address 23

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

3.2.2.6. Wildcard Domain Validation 23
3.2.2.7. Data Source Accuracy 23
3.2.2.8. CAA Records 23
3.2.3. Authentication of Individual Identity 24
3.2.4. Non-Verified Subscriber Information 24
3.2.5. Validation of Authority 24
3.2.6. Criteria for Interoperation or Certification 24
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 24
3.3.1. Identification and Authentication for Routine Re-Key 24
3.3.2. Identification and Authentication for Re-Key After Revocation 24
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 24

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 25

4.1. CERTIFICATE APPLICATION 25
4.1.1. Who Can Submit a Certificate Application 25
4.1.2. Enrollment Process and Responsibilities 25
4.2. CERTIFICATE APPLICATION PROCESSING 25
4.2.1. Performing Identification and Authentication Functions 25
4.2.2. Approval or Rejection of Certificate Applications 26
4.2.3. Time to Process Certificate Applications 26
4.3. CERTIFICATE ISSUANCE 27
4.3.1. CA Actions during Certificate Issuance 27
4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate 27
4.4. CERTIFICATE ACCEPTANCE 27
4.4.1. Conduct Constituting Certificate Acceptance 27
4.4.2. Publication of the Certificate by the CA 27
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 27
4.5. KEY PAIR AND CERTIFICATE USAGE 27
4.5.1. Subscriber Private Key and Certificate Usage 27
4.5.2. Relying Party Public Key and Certificate Usage 28
4.6. CERTIFICATE RENEWAL 28
4.6.1. Circumstance for Certificate Renewal 28
4.6.2. Who May Request Renewal 28
4.6.3. Processing Certificate Renewal Requests 28
4.6.4. Notification of New Certificate Issuance to Subscriber 28
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 28
4.6.6. Publication of the Renewal Certificate by the CA 28
4.6.7. Notification of Certificate Issuance by the CA to Other Entities 28
4.7. CERTIFICATE RE-KEY 28
4.7.1. Circumstance for Certificate Re-Key 28
4.7.2. Who May Request Certification of a New Public Key 29
4.7.3. Processing Certificate Re-Keying Requests 29
4.7.4. Notification of New Certificate Issuance to Subscriber 29
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 29

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.7.6. Publication of the Re-Keyed Certificate by the CA 29
4.7.7. Notification of Certificate Issuance by The CA to Other Entities 29
4.8. CERTIFICATE MODIFICATION 29
4.8.1. Circumstance for Certificate Modification 29
4.8.2. Who May Request Certificate Modification 29
4.8.3. Processing Certificate Modification Requests 29
4.8.4. Notification of New Certificate Issuance to Subscriber 29
4.8.5. Conduct Constituting Acceptance of Modified Certificate 29
4.8.6. Publication of The Modified Certificate by the CA 29
4.8.7. Notification of Certificate Issuance by The CA to Other Entities 29
4.9. CERTIFICATE REVOCATION AND SUSPENSION 29
4.9.1. Circumstances for Revocation 29
4.9.2. Who Can Request Revocation 31
4.9.3. Procedure for Revocation Request 31
4.9.4. Revocation Request Grace Period 32
4.9.5. Time within which CA Must Process the Revocation Request 32
4.9.6. Revocation Checking Requirement for Relying Parties 32
4.9.7. CRL Issuance Frequency 32
4.9.8. Maximum Latency for CRLs 33
4.9.9. Online Revocation/Status Checking Availability 33
4.9.10. Online Revocation Checking Requirements 33
4.9.11. Other Forms of Revocation Advertisements Available 33
4.9.12. Special Requirements Related to Key Compromise 33
4.9.13. Circumstances for Suspension 33
4.9.14. Who Can Request Suspension 33
4.9.15. Procedure for Suspension Request 33
4.9.16. Limits on Suspension Period 34
4.10. CERTIFICATE STATUS SERVICES 34
4.10.1. Operational Characteristics 34
4.10.2. Service Availability 34
4.10.3. Optional Features 34
4.11. END OF SUBSCRIPTION 34
4.12. KEY ESCROW AND RECOVERY 34
4.12.1. Key Escrow and Recovery Policy and Practices 34
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 34

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 35

5.1. PHYSICAL SECURITY CONTROLS 35
5.1.1. Site Location and Construction 35
5.1.2. Physical Access 36
5.1.3. Power and Air Conditioning 36
5.1.4. Water Exposures 36
5.1.5. Fire Prevention and Protection 36
5.1.6. Media Storage 36
5.1.7. Waste Disposal 37

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.1.8. Off-Site Backup 37
5.2. PROCEDURAL CONTROLS 37
5.2.1. Trusted Roles 37
5.2.2. Number of Persons Required per Task 38
5.2.3. Identification and Authentication for Each Role 38
5.2.4. Roles Requiring Separation of Duties 38
5.3. PERSONNEL CONTROLS 38
5.3.1. Qualifications, Experience, and Clearance Requirements 38
5.3.2. Background Check Procedures 38
5.3.3. Training Requirements 38
5.3.4. Retraining Frequency and Requirements 39
5.3.5. Job Rotation Frequency and Sequence 39
5.3.6. Sanctions for Unauthorized Actions 39
5.3.7. Independent Contractor Controls 39
5.3.8. Documentation Supplied to Personnel 39
5.4. AUDIT LOGGING PROCEDURES 39
5.4.1. Types of Events Recorded 39
5.4.2. Frequency of Processing Log 40
5.4.3. Retention Period for Audit Log 41
5.4.4. Protection of Audit Log 41
5.4.5. Audit Log Backup Procedures 41
5.4.6. Audit Collection System (internal vs. external) 41
5.4.7. Notification to Event-Causing Subject 41
5.4.8. Vulnerability Assessments 41
5.5. RECORDS ARCHIVAL 42
5.5.1. Types of Records Archived 42
5.5.2. Retention Period for Archive 42
5.5.3. Protection of Archive 42
5.5.4. Archive Backup Procedures 42
5.5.5. Requirements for Time-Stamping of Records 42
5.5.6. Archive Collection System (Internal or External) 42
5.5.7. Procedures to Obtain and Verify Archive Information 42
5.6. KEY CHANGEOVER 43
5.7. COMPROMISE AND DISASTER RECOVERY 43
5.7.1. Incident and Compromise Handling Procedures 43
5.7.2. Computing Resources, Software, and/or Data are Corrupted 43
5.7.3. Entity Private Key Compromise Procedures 44
5.7.4. Business Continuity Capabilities after a Disaster 44
5.8. CA OR RA TERMINATION 45
6. TECHNICAL SECURITY CONTROLS 45
6.1. KEY PAIR GENERATION AND INSTALLATION 45
6.1.1. Key Pair Generation 45
6.1.2. Private Key Delivery to Subscriber 46
6.1.3. Public Key Delivery to Certificate Issuer 46

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

6.1.4. CA Public Key Delivery to Relying Parties 46
6.1.5. Key Sizes 46
6.1.6. Public Key Parameters Generation and Quality Checking 46
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field) 46
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 46
6.2.1. Cryptographic Module Standards and Controls 46
6.2.2. Private Key Multi-Person Control 47
6.2.3. Private Key Escrow 47
6.2.4. Private Key Backup 47
6.2.5. Private Key Archival 47
6.2.6. Private Key Transfer into or From a Cryptographic Module 47
6.2.7. Private Key Storage on Cryptographic Module 48
6.2.8. Method of Activating Private Keys 48
6.2.9. Method of Deactivating Private Keys 48
6.2.10. Method of Destroying Private Keys 48
6.2.11. Cryptographic Module Rating 48
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 48
6.3.1. Public Key Archival 48
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 48
6.4. ACTIVATION DATA 49
6.4.1. Activation Data Generation and Installation 49
6.4.2. Activation Data Protection 49
6.4.3. Other Aspects of Activation Data 49
6.5. COMPUTER SECURITY CONTROLS 49
6.5.1. Specific Computer Security Technical Requirements 49
6.5.2. Computer Security Rating 49
6.6. LIFE CYCLE TECHNICAL CONTROLS 49
6.6.1. System Development Controls 49
6.6.2. Security Management Controls 50
6.6.3. Life Cycle Security Controls 50
6.7. NETWORK SECURITY CONTROLS 51
6.8. TIME-STAMPING 52

7. CERTIFICATE, CRL AND OCSP PROFILES 52

7.1. CERTIFICATE PROFILE 52
7.1.1. Version Number(s) 52
7.1.2. Certificate Content and Extensions 52
7.1.3. Algorithm Object Identifiers 53
7.1.4. Name Forms 53
7.1.5. Name Constraints 53
7.1.6. Certificate Policy Object Identifier 53
7.1.7. Usage of Policy Constraints Extension 53
7.1.8. Policy Qualifiers Syntax and Semantics 53
7.1.9. Processing Semantics for the Critical Certificate Policies Extension 53
7.2. CRL PROFILE 54

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

7.2.1. Version Number(s) 54
7.2.2. CRL and CRL Entry Extensions 54
7.3. OCSP PROFILE 55
7.3.1. Version Number(s) 55
7.3.2. OCSP Extensions 55
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 56
8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 56
8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR 56
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 56
8.4. TOPICS COVERED BY ASSESSMENT 56
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY 57
8.6. COMMUNICATION OF RESULTS 57
8.7. SELF-AUDITS 57
9. OTHER BUSINESS AND LEGAL MATTERS 57
9.1. FEES 57
9.1.1. Certificate Issuance or Renewal Fees 57
9.1.2. Certificate Access Fees 57
9.1.3. Revocation or Status Information Access Fees 57
9.1.4. Fees for Other Services 58
9.1.5. Refund Policy 58
9.2. FINANCIAL RESPONSIBILITY 58
9.2.1. Insurance Coverage 58
9.2.2. Other Assets 58
9.2.3. Insurance or Warranty Coverage for End-Entities 58
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION 58
9.3.1. Scope of Confidential Information 58
9.3.2. Information Not Within the Scope of Confidential Information 58
9.3.3. Responsibility to Protect Confidential Information 58
9.4. PRIVACY OF PERSONAL INFORMATION 58
9.4.1. Privacy Plan 58
9.4.2. Information Treated as Private 59
9.4.3. Information Not Deemed Private 59
9.4.4. Responsibility to Protect Private Information 59
9.4.5. Notice and Consent to Use Private Information 59
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 59
9.4.7. Other Information Disclosure Circumstances 59
9.5. INTELLECTUAL PROPERTY RIGHTS 59
9.6. REPRESENTATIONS AND WARRANTIES 59
9.6.1. CA Representations and Warranties 59
9.6.2. RA Representations and Warranties 60
9.6.3. Subscriber Representations and Warranties 61
9.6.4. Relying Party Representations and Warranties 62
9.6.5. Representations and Warranties of Other Participants 62

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

9.7. DISCLAIMERS OF WARRANTIES 62
9.8. LIMITATIONS OF LIABILITY 62
9.9. INDEMNITIES 63
9.10. TERM AND TERMINATION 63
9.10.1. Term 63
9.10.2. Termination 63
9.10.3. Effect of Termination and Survival 63
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 63
9.12. AMENDMENTS 63
9.12.1. Procedure for Amendment 63
9.12.2. Notification Mechanism and Period 64
9.12.3. Circumstances under Which OID Must Be Changed 64
9.13. DISPUTE RESOLUTION PROVISIONS 64
9.14. GOVERNING LAW 64
9.15. COMPLIANCE WITH APPLICABLE LAW 64
9.16. MISCELLANEOUS PROVISIONS 64
9.16.1. Entire Agreement 64
9.16.2. Assignment 64
9.16.3. Severability 64
9.16.4. Enforcement (attorneys' fees and waiver of rights) 64
9.16.5. Force Majeure 65
9.17. OTHER PROVISIONS 65
APPENDIX-A: OV SSL CERTIFICATE PROFILE 66

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

1. INTRODUCTION

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

Referred as Certificate Policy and Certification Practice Statement (CP/CPS), this combined document has been prepared in compliance with the guidebook of "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" for the purpose of describing the working principles and practices related to the Kamu SM's Organization Validated SSL (OV SSL) certification to organizations located in Republic of Turkey.

Kamu SM conforms to the current version of the "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted TLS Server Certificates" published at https://www.cabforum.org. Besides, the CP/CPS describes the practices used to comply with the current versions of the following policies, guidelines and requirements:

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- CA/Browser Forum Network and Certificate System Security Requirements
- CCADB Policy
- Microsoft Trusted Root Program Requirements
- Mozilla Root Store Policy
- Apple Root Certificate Program
- Chrome Root Program Policy
- 360 Browser CA Policy

In the event of any inconsistency between the CP/CPS document and these documents, the requirements set out in respective documents take precedence over this document.

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

1.1. OVERVIEW

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

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

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

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

1.2. DOCUMENT NAME AND IDENTIFICATION

Document Name: Kamu SM SSL Certificate Policy and Certification Practice Statement

Version: 3.11.1

Release Date: 14.10.2026

OID: 2.16.792.1.2.1.1.5.7.1.3

Date	Changes	Version
30.03.2016	- Initial Release	**1.0.0**
07.03.2017	- Section 3.2.2 Authentication of Organization Identity was elaborated. - Version history was added. - Certificate profile was updated (serial number). - Section 4.9.3 SSL Certificate Revocation Form was referenced.	**1.0.1**
17.04.2017	- Section 3.2.2 Authentication of Organization Identity is updated. - Updates via annually updates of CP/CPS in April 2017	**2.1.1**
20.06.2017	- CAA records examination added.	**2.2.1**
25.09.2017	- Updates are done according to CA/B BR 1.5.0.	**3.0.0**
21.10.2017	- In domain validation, meta tag usage is replaces with file usage.	**3.1.0**
26.01.2018	- According to BR Self Assessment, minor changes are done. - Section 3.2.2 is updated with CAA Errata 5065.	**3.2.0**

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

07.07.2018	- ECC is added to public key algorithms.	**3.2.1**
24.10.2018	- Updates are done according to new audit standard ETSI EN 319 411-1. - Updates are done according to CA/B BR 1.6.1.	**3.3.0**
16.10.2019	- Updates within the scope of annual CPS revision.	**3.3.1**
11.06.2020	- 3.2.2.4.6 Domain validation method is changed with 3.2.2.4.18.	**3.3.2**
04.09.2020	- Issued on or after 1 September 2020, SSL certificate lifetime is reduced to 398 days.	**3.3.3**
16.07.2021	- The acceptable methods that can be used by third parties as proof of key compromise are defined in Section 4.9.12. - Updates are done according to CA/B BR 1.7.6.	**3.3.4**
10.09.2021	- Updates are done according to new audit standard ETSI EN 319 411-1 v.1.3.1.	**3.4.0**
01.12.2021	- 3.2.2.4.18 Domain validation method is changed with 3.2.2.4.4 and 3.2.2.4.7. - The use of the subject:organizationalUnitName field in subscriber certificates has been deprecated.	**3.5.0**
04.07.2022	- The use of the subject:Locality field in subscriber certificates has been deprecated. - Revocation reasons for end-entity certificates have been clarified.	**3.6.0**
26.08.2022	- Updates are done within the scope of merging the SSL Application Form and SSL Subscriber Agreement.	**3.6.1**
16.08.2023	- Within the scope of annual revision, minor editorial changes are done throughout the document for consistency. - CRLReasonCodes of revocations reasons are specified.	**3.6.2**
04.09.2023	- SSL certificate profile is updated according to CA/B BR.	**3.6.3**
13.12.2023	- Updates are done within the scope of issuing SSL certificates for domain names ending with ".tr" ccTLD. - Changes are done in line with the Self-Assessment. - CP and CPS documents are combined.	**3.7.0**
29.04.2024	- Router and firewall activities logging requirements are detailed. - The profile of new subordinate certificate in accordance with CA/B BR 2.0.0 has been added. Within the scope of the changes into the profile, arrangements are done in the relevant sections. - Updates are done about use of delegated third parties for domain control validation.	**3.8.0**
08.10.2024	- In line with current ETSI EN 319 411-1, the process to be followed regarding the conformation of the revocation request has been clarified. - Weak key controls have been extended. - The statements regarding pre-issuance and post-issuance linting have been clarified.	**3.8.1**

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

	- Arrangements have been made within the scope of internal audit.	
08.04.2025	- Updates are done within the scope of Multi-Perspective Issuance Corroboration. - Information about mass revocation event has been added.	**3.9.0**
17.06.2025	- Updates are done to extend the scope of OV SSL Certification Service.	**3.10.0**
09.03.2026	- The maximum validity period of certificate has been updated. - Compliance with the CCADB Policy has been explicitly stated. - Statements indicating that the DNSSEC validation is performed on DNS queries have been added.	**3.10.1**
15.04.2026	- Relevant sections have been revised to reflect the cross-certification model.	**3.11.0**
14.10.2026	- Information related to the certificate, CRL and OCSP profiles, as well as recorded activities, has been updated to more comprehensively reflect existing practices.	**3.11.1**

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

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

1.3. PKI PARTICIPANTS

PKI Participants defined within the scope of this document are the parties bearing relevant rights and obligations within certification services of Kamu SM.

These parties are defined as CA, registration authority, Subscribers and relying parties. All CA services are carried out by Kamu SM personnel.

1.3.1. Certification Authorities

Kamu SM, as a CA, is responsible for the management of the certificate lifecycle, including application processing, certificate issuance, renewal, distribution, and revocation. Kamu SM provides OV SSL certificate services.

The PKI hierarchy managed by Kamu SM consists of a Root and Subordinate Certification Authorities. Where necessary, cross certificates may be issued to ensure continuity of trust and interoperability.

- **Root Certificate:** The trust anchor at the top of the hierarchy responsible for issuing and signing Subordinate CA Certificates.
- **Cross Certificate:** A certificate that may be issued by the currently trusted Root Certificate to support compatibility or transition scenarios within the certificate hierarchy.
- **Subordinate CA Certificate:** A certificate responsible for issuing end-entity certificates.

In line with current industry requirements, cross-certification may be used within the Kamu SM SSL certificate hierarchy to ensure a seamless transition. Cross Certificates are subject to the same

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

technical, operational, and security requirements applicable to Subordinate CA Certificates under this CP/CPS.

Kamu SM provides revocation services through OCSP and CRL for subordinate CA certificates, (where applicable) cross certificates, and end-entity SSL certificates. The revocation status of the cross certificate is determined via the CRL and/or OCSP services published by the issuing Root CA. Revocation checking for end-entity certificates is performed through the relevant subordinate CA.

1.3.2. Registration Authorities

Registration units execute services such as certificate application and revocation process intended for end users. This unit creates the first customer record and executes required identification and authentication processes and directs relevant certificate requests to certificate issuance unit.

All registration procedures are directly executed by Kamu SM personnel. Kamu SM does not use a Delegated Third Party to perform of all or any part of requirements in Section 3.2.

1.3.3. Subscribers

Legal entities whose certificates are issued by Kamu SM and which are responsible for using their certificates in compliance with this CP/CPS.

1.3.4. Relying Parties

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

1.3.5. Other Participants

Not applicable.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

This CP/CPS applies exclusively to certificates intended for the SSL/TLS server authentication trust purpose (serverAuthentication: id-kp-serverAuth (1.3.6.1.5.5.7.3.1)).

SSL certificates issued by Kamu SM are intended to be used for authenticating a server to clients and for establishing encrypted communication between the server and the client.

An SSL certificate may only be used on servers providing services for the domain name specified in the certificate. The rights to use the certificates belong solely to the Subscribers.

1.4.2. Prohibited Certificate Uses

The permitted use of certificates is restricted by the “Key Usage” and “Extended Key Usage” extensions included in the certificate. SSL certificate issued by Kamu SM shall not be used for any purposes those specified in these extensions.

A certificate does not by itself guarantee that the Subject is trustworthy, safe to do business with, or compliant with applicable laws. A certificate only confirms that the information contained in the certificate was verified in accordance with this CP/CPS at the time of issuance.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

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

1.5.2. Contact Person

Requests for information associated with this CP/CPS document should be addressed to the following contact information of Kamu SM:

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

Phone : (+90) 444 5 576

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

E-Mail : bilgi@kamusm.gov.tr

Problem Reporting E-Mail: kamusm.cainfo@tubitak.gov.tr

URL : https://kamusm.bilgem.tubitak.gov.tr

1.5.3. Person Determining CPS Suitability for the Policy

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

1.5.4. CPS Approval Procedure

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

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

Applicant: A legal entity that applies for a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber.

Applicant Representative: A natural person authorized by the applicant organization and assigned to carry out the SSL certificate processes on behalf of the organization.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates.

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

Cross Certificate: A certificate that is used to establish a trust relationship between two CAs.

CSPRNG: A random number generator intended for use in a cryptographic system.

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

Kamu Sertifikasyon Merkezi (Kamu SM): A TÜBİTAK unit providing certification services for organizations located in Turkey.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

Key Pair: Private Key and its associated Public Key.

Mass Revocation Event: The revocation of a substantial number of certificates within a relatively short timeframe due to a common cause, compliance requirement, or security incident.

Multi-Perspective Issuance Corroboration (MPIC): A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

Network Perspective: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check.

Object Identifier (OID): A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

Online Certificate Status Protocol (OCSP): An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.

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

Precertificate: A precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined in RFC 6962.

Primary Network Perspective: The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Qualified Auditor: A natural person or legal entity that performs conformity audits under the accreditation in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403.

Qualified Electronic Certificate: Electronic certificate which is defined by Electronic Signature Law No. 5070 of Republic of Turkey, applicable for Electronic Signatures/Seals in terms of technical considerations.

Quorum: A set of validation results obtained from the required number of distinct Network Perspectives used to corroborate the determinations made by the Primary Network Perspective as part of Multi-Perspective Issuance Corroboration.

Random Value: A value specified by Kamu SM to the Applicant that exhibits at least 112 bits of entropy.

Relying Parties: Any natural person or legal entity that relies on a Certificate.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policy and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

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

Root CA Certificate: Self-signed certificate issued by the Root CA.

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

Subordinate CA Certificate: Certificate of the Subordinate CA.

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

Subscriber: A legal entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

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

Trade Name: Officially registered name under which a merchant or company conducts its business activities.

Wildcard SSL: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Working Day: Weekdays except national holidays and the weekend.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

1.6.2. Acronyms

ADN: Authorization Domain Name

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

CA: Certificate Authority

CAA: Certificate Authority Authorization

CCADB: Common CA Database

ccTLD: Country Code Top-Level Domain

CEN: European Committee for Standardization

CP/CPS: Certificate Policy and Certification Practice Statement

CRL: Certificate Revocation List

CSR: Certificate Signing Request

CWA: CEN Workshop Agreement

DBA: Doing Business As

DETSİS: Central Registration System of the State Organization

DNS: Domain Name System

DNSSEC: Domain Name Security Extensions

EAL: Evaluation Assurance Level

ECC: Elliptic Curve Cryptography

ETSI EN: ETSI European Standard

ETSI TS: ETSI Technical Specifications

ETSI: European Telecommunications Standards Institute

FIPS PUB: Federal Information Processing Standards Publications

FQDN: Fully-Qualified Domain Name

IETF RFC: Internet Engineering Task Force Request for Comments

ISO/IEC: International Organisation for Standardization/International Electrotechnical Commission

ITU: International Telecommunication Union

Kamu SM: Government Certification Authority of Turkey

NIST: (US Government) National Institute of Standards and Technology

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PKI: Public Key Infrastructure

SAN: Subject Alternative Name

SHA: Secure Hash Algorithm

SSL: Secure Socket Layer

TLD: Top Level Domain

UTC: Coordinated Universal Time

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

A repository is an environment in which the documents such as root, subordinate CA and cross certificates (if any) of Kamu SM, revocation status information, CP/CPS documents, Application Form and Subscriber Agreements are publicly, securely and freely published through an appropriate and readily accessible online means that is available on a 24x7 basis.

Documents published in the repository are updated when necessary. Such updates are indicated by version numbers and update dates included in the revised documents.

2.1. REPOSITORIES

Kamu SM repository is accessible over https://kamusm.bilgem.tubitak.gov.tr and http://depo.kamusm.gov.tr/ilke.

Kamu SM does not employ a Delegated Third Party to operate the repository.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The following information is available in the repository to be accessed publicly:

- Root, subordinate CA and cross certificates (if any) of Kamu SM,
- Hash values of certificates of Kamu SM and hash algorithms used in the calculation of hash values,
- OID list used by Kamu SM,
- Kamu SM CP/CPS documents,
- Forms and Agreements,
- Up to date revocation status records

English and Turkish versions of the SSL Application Form and Subscriber Agreement and CP/CPS document are internationally available in the Kamu SM's website.

Older versions of CP/CPS documents can be accessed via the following link: https://kamusm.bilgem.tubitak.gov.tr/depo/ilke_ve_uygulama_esaslari/eski_ilke_ve_uygulama_esaslari.jsp

SSL web pages which are serviced by Kamu SM in order to allow application software suppliers to test their software are given below:

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

2.3. TIME OR FREQUENCY OF PUBLICATION

The changes on CP/CPS document are reflected Forms and Agreements. Updated documents are published in the repository as soon as possible.

Certificates of Kamu SM are published in the repository as soon as possible after issuance.

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

Kamu SM reviews and updates its CP/CPS document at least once every year so that its operations remain accurate and comply with the external requirements specified by the international organizations such as ETSI and CA/B Forum. Kamu SM monitors updates to the ETSI EN 319 401, ETSI EN 319 411-1, CA/B Forum Baseline Requirements standards, CCADB Policy and Root Programs, and implements the necessary updates to its operations and make changes in the CP/CPS document in a timely manner.

2.4. ACCESS CONTROLS ON REPOSITORIES

Kamu SM repository is publicly available in a read-only manner. Updating repository is carried out by authorized Kamu SM personnel.

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

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

3. IDENTIFICATION AND AUTHENTICATION

Kamu SM verifies the organization identity, authenticity of Applicant Representative's certificate request and domain ownership of the Applicant. Kamu SM performs verification process according to legal and technical requirements based on all necessary documents and official resources.

3.1. NAMING

3.1.1. Types of Names

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

3.1.2. Need for Names to be Meaningful

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

3.1.3. Anonymity or Pseudonymity of Subscribers

Anonymity or pseudonymity of the Subscriber is not allowed.

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

Organization identity information in the content of certificates issued by Kamu SM are distinctive for each organization. Availability of only domain names, virtual server names or internal server names and IP addresses without agency information are not permitted within the certificate.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

Kamu SM issues OV SSL certificates to only organizations located in Turkey. The following is included in OV SSL certificates:

- "CN (Common Name)" field:
  - Name of server registered on behalf of the Subscriber organization in DNS is written in "CN" field.
  - "*.<domain name>" is written in this field in OV SSL wildcard certificates. This field does not contain non-distinctive names such as "*.com" or "*.com.tr".
  - IP address or internal server name is not written in this field.
- "O (Organization)" field contains the open title or understandably abbreviated form of the Subscriber organization as laid down;
  - In organizational law or other legislation or,
  - Reliable data sources (DETSİS, Turkish Trade Registry Gazette, etc.) recognized by Kamu SM.
- "ST (State or Province)" field contains province information where the Subscriber organization is located.
- "C (Country)" field includes country code (TR) contained in ISO 3166-1 Alpha-2 standard of the country where the Subscriber organization is located.
- Name of server registered on behalf of the Subscriber organization in DNS contained in "CN" field is also written in "SAN" field. Several domain names can be written in certificates provided that each domain name belongs to the Applicant or is under its control.

3.1.6. Recognition, Authentication, and Role of Trademarks

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

3.2. INITIAL IDENTITY VALIDATION

During the initial identity validation, the methods specified in the following subheadings shall be applied by Kamu SM.

3.2.1. Method to Prove Possession of Private Key

Certificate signing request created by the Applicant shall be signed by a private key. Kamu SM validates the signature of the CSR file. In this way, it is proven that the Applicant possess the private key.

3.2.2. Authentication of Organization and Domain Identity

The identity and address of the organization are verified according to governmental databases and legal documents. Organization identity is verified as defined in Section 3.2.2.1. Domain authorization is validated using the methods defined in Section 3.2.2.4. Kamu SM conducts the authentication of organization and domain identity process in accordance with internal policies and procedures that are regularly updated in order to comply with the BRs.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

3.2.2.1. Identity

Identity and address verification steps:

- The identity (title, legal existence, business presence, etc.) and address of the Applicant is verified according to governmental databases that are periodically updated. In addition, it is checked that the application form approved by the Applicant.
- The identity and address of the Applicant is checked whether it is same as the information in the certificate signing request and the application form.

3.2.2.2. DBA/Tradename

Kamu SM verifies the tradenames and/or DBAs to be included in certificates using reliable source or official records.

3.2.2.3. Verification of Country

Kamu SM only issues certificates to organizations located in Turkey with domain names ending with ".tr" ccTLD.

3.2.2.4. Validation of Domain Authorization or Control

Domain ownership verification steps:

- First, it is checked whether the domain name ends with ".tr" ccTLD.
- It is also checked whether the domain name specified in the application form is the same as the domain name in the certificate signing request.
- Kamu SM uses one of the following methods to test the Applicant's control over the domain name:
  - ***Constructed E-mail to Domain Contact (BR Section 3.2.2.4.4):***
    - Kamu SM sends an e-mail including a random value to one of the e-mail addresses of the DNS mail server (*admin@domainname, administrator@domainname, webmaster@domainname, hostmaster@domainname, postmaster@domainname*).
    - After receiving a confirming response utilizing the random value Kamu SM verify the domain ownership.
    - Kamu SM checks the random value and domain ownership is verified.
    - The random value is unique in each e-mail and remains valid for use in a confirming response for no more than 30 (thirty) days from its creation.
    - The email may be re-sent in its entirety, including the re-use of the random value, provided that its entire contents and recipient shall remain unchanged.
  - ***DNS Change (BR Section 3.2.2.4.7):***
    - The Applicant creates a DNS TXT or CNAME record using the random value specified by Kamu SM.
    - Kamu SM checks the presence of the random value in DNS record and domain ownership is verified.
    - The random value is unique to the certificate request and not used after 30 (thirty) days.
    - Kamu SM uses MPIC detailed in CA/B BR Section 3.2.2.9 for this method.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

The methods defined in CA/B BR Section 3.2.2.4.4 and 3.2.2.4.7 are used for domain ownership validation and control. The relevant version of BR and the method used during the domain ownership and control validation process are recorded.

Effective March 15th 2026; Kamu SM performs DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective as defined in CA/B BR Section 3.2.2.4.

3.2.2.5. Authentication for an IP Address

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

3.2.2.6. Wildcard Domain Validation

In wildcard certificate validation, it is first checked that FQDN does not contain "*" on the left side of high-level top domain such as "*.com" or "*.com.tr". To verify domain name ownership for wildcard certificates, all controls specified in Section 3.2.2.4 are applied.

3.2.2.7. Data Source Accuracy

Kamu SM evaluates the validation data sources for its reliability and accuracy. All applications made to Kamu SM shall be supported by legal documents sufficient to authenticate the required Subject Identity Information. However, where such documents and related validation data have been previously collected and validated in accordance with Section 4.2.1, Kamu SM may reuse such information, provided that the applicable conditions and time limitations are satisfied.

The application shall include the following information, some of will be included in the Subject field or the certificate:

- Legal name of the organization (Included in the O field)
- Address of the organization (Province included in the ST field)
- Tax number
- Applicant Representative information
- Domain name(s) (Included in the CN and SAN fields)
- Information about the authorized person approving the certificate application
- PKCS#10 Certificate Signing Request (CSR)

All required information must be provided during the application process. Upon receipt of the application, Kamu SM performs validation in two main stages. First, the identity and address of the organization are verified according to governmental data sources and legal documents. Second, the domain ownership or control of Applicant is verified in accordance with Section 3.2.2.4.

Subject Identity validation data may be reused only in accordance with conditions specified in Section 4.2.1. Domain validation is performed for each certificate issuance and is not subject to reuse. Both validation procedure conforms to CA/B Forum the BRs.

3.2.2.8. CAA Records

As part of the issuance process, Kamu SM checks CAA records for all domains listed in the certificate according to the procedure in RFC 8659 (DNS Certification Authority Authorization (CAA) Resource Record). "kamusm.gov.tr" domain name is recognized in a CAA record's *issue* and *issuewild* property

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

tags. If there exists no problem in CAA record, the certificate is issued within the TTL of CAA record, or 8 hours, whichever is greater. In the case of lookup failure, the certificate can be issued if the failure is outside Kamu SM's infrastructure or the lookup has been re-tried at least once. Each CAA record is logged whether the certificate is issued or not issued.

Kamu SM uses Multi-Perspective Issuance Corroboration detailed in CA/B BR Section 3.2.2.9 for checking CAA records.

Effective March 15th 2026; Kamu SM performs DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS queries associated with the CAA record lookups performed by the Primary Network Perspective as defined CA/B BR Section 3.2.2.8.1.

3.2.3. Authentication of Individual Identity

Only organizational application is accepted since Kamu SM offers OV SSL service only to organizations.

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

The Applicant specifies the Applicant Representative who may carries out the SSL certificate application process on behalf of the organization. Kamu SM shall not accept any certificate request that are outside this specification.

Applicant Representative executing application procedures is verified by the legal documents whether it has right to apply on behalf of the agency. Through the phone numbers verified according to this, it is requested to confirm the application by calling the Applicant Representative.

3.2.6. Criteria for Interoperation or Certification

Kamu SM can provide cross certification service within its own CA infrastructure, for purposes such as root renewal transition. All cross-signed CA certificates issued in this scope are published in Kamu SM repository.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-Key

Certificate re-key requests for SSL certificates are treated as new certificate application. Identification and authentication procedures are applied as described in Section 3.2.

3.3.2. Identification and Authentication for Re-Key After Revocation

Re-key requests after revocation of a certificate are treated as new certificate application. Identification and authentication procedures are applied as described in Section 3.2.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

Who can apply for certificate revocation is defined in Section 4.9.2.

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Organizations located in Turkey can apply to Kamu SM for SSL certificate. These applications shall be made corporately by an organization employee duly authorized. The agency makes an application by filling out the SSL Certificate Application Form and Subscriber Agreement to be downloaded from Kamu SM website. Signed and sealed/stamped form shall be sent to Kamu SM. Electronically signed/sealed application forms created using qualified electronic certificates are also accepted. Organization employee may not individually make an application without the request of the organization. Kamu SM may request additional documents to verify the identity of the organization and the applicant representative.

4.1.2. Enrollment Process and Responsibilities

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

- It shall send the signed and sealed/stamped SSL Certificate Application Form and Subscriber Agreement as incorporating all necessary information to Kamu SM. In case additional documents are requested to verify the identity of the organization and the applicant representative, it also shall send. The Applicant shall be liable for following up the information sent to Kamu SM and notifying Kamu SM in case of modification in this information.
- The Applicant shall generate key pair by itself and shall create Certificate Signing Request (CSR) as to prove that private key belongs to itself and sends this to Kamu SM from corporate e-mail address.
- The Applicant shall take all required measures for protecting the confidentiality and integrity of its private key.

Applicant shall submit sufficient information to allow Kamu SM to successfully perform the verification process. Kamu SM can request additional documentation if deemed necessary.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

SSL applications shall be executed in pursuance of the principles set out in Section 3.2 and 4.1 and the related procedures of Kamu SM. No Delegated Third Party is authorized by Kamu SM in performing identification and authentication functions.

Kamu SM may rely on documents and data collected and validated pursuant to Section 3.2 for the purpose of validating Subject Identity Information, or may reuse previously validated Subject Identity

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

Information data. However, Kamu SM reserves the right to perform a new organizational validation whenever it deems necessary.

Where Subject Identity Information validation data is reused, Kamu SM shall ensure that the Subject Identity Information validation data relied upon was collected and validated no more than 398 days prior to issuing the Certificate.

Domain ownership or control validation performed under Section 3.2.2.4 shall be repeated prior to each certificate issuance and is not subject to any reuse period.

Kamu SM can use additional methods for authentication of high-risk certificate requests.

Kamu SM checks CAA records for all domains listed in the certificate according to the procedure in RFC 8659. Policy on processing CAA DNS Records is given in Section 3.2.2.8.

4.2.2. Approval or Rejection of Certificate Applications

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

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

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

Kamu SM does not issue SSL certificates containing IP Addresses and internal domain names.

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

4.2.3. Time to Process Certificate Applications

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

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

Certificate applications accepted in pursuance of the principles contained in Section 4.2.2 shall be processed by Kamu SM and certificate shall be issued following verification of CSR file. Prior and after signing the certificate, pre-issuance and post-issuance linting are performed for checking compliance with the applicable standards and the OV SSL Certificate Profile in Appendix-A. All the steps during this procedure are logged.

Certificates issued by root CA can only be generated by direct command of the personnel authorized by the CA in accordance with internal policies and procedures.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

Kamu SM shall send the certificate to Applicant Representative's corporate e-mail address which was provided during the enrolment process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

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

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

4.4.2. Publication of the Certificate by the CA

Kamu SM's root, subordinate CA and cross certificates (if any) are published in its own repository. End-entity SSL certificates are published by delivering them to the Subscriber.

Before an SSL certificate is issued, its corresponding precertificate is submitted to one or more Certificate Transparency (CT) log servers.

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

No stipulation.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscriber shall use its certificate and private key within the framework of the terms and conditions contained in the SSL Certificate Application Form and Subscriber Agreement and in CP/CPS document with other regulations and standards being subjected to. Subscriber shall install the SSL certificate only on servers that are accessible at the "Subject Alternative Name" listed in the certificate.

Subscriber shall be liable for taking all reasonable measures to assure control of, keep confidential, and properly protect at all times its private key. Private key corresponding to SSL certificate may only be used within the purposes specified in the "Key Usage" and "Extended Key Usage" fields of the certificate.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.5.2. Relying Party Public Key and Certificate Usage

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

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

4.6. CERTIFICATE RENEWAL

Certificate renewal means the issuance of a new certificate with a new validity period using the same key pair and Subject information after the expiration of the previous certificate.

Kamu SM does not perform certificate renewal for SSL certificates. Certificate renewal requests are processed as new certificate request. Identification and authentication procedures are applied as described in Section 3.2.

4.6.1. Circumstance for Certificate Renewal

Kamu SM does not perform certificate renewal for SSL certificates.

4.6.2. Who May Request Renewal

No stipulation.

4.6.3. Processing Certificate Renewal Requests

No stipulation.

4.6.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

No stipulation.

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

No stipulation.

4.7. CERTIFICATE RE-KEY

Certificate re-key means the issuance of a new certificate that certifies a new public key without changing the Subscriber information contained in the Subject field of the certificate.

Kamu SM does not perform certificate re-key as a separate process for SSL certificates. Request involving a new key pair are processed as new certificate request. Identification and authentication procedures are applied as described in Section 3.2.

4.7.1. Circumstance for Certificate Re-Key

Requests involving a new key pair are processed as new certificate requests. Procedures defined for initial certificate issuance apply.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.7.2. Who May Request Certification of a New Public Key

Subscriber and/or the Applicant Representative are authorized to request certificate issuance.

4.7.3. Processing Certificate Re-Keying Requests

Procedures defined for initial certificate issuance apply.

4.7.4. Notification of New Certificate Issuance to Subscriber

Procedures defined in Section 4.3.2 apply.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Procedures defined in Section 4.4.1 apply.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Procedures defined in Section 4.4.2 apply.

4.7.7. Notification of Certificate Issuance by The CA to Other Entities

No stipulation.

4.8. CERTIFICATE MODIFICATION

In case of modification within the information in the content of a certificate issued by Kamu SM, the certificate shall be revoked and an application shall be made for a new certificate together with new information. Certificate modification requests are processed as new certificate request.

4.8.1. Circumstance for Certificate Modification

No stipulation.

4.8.2. Who May Request Certificate Modification

No stipulation.

4.8.3. Processing Certificate Modification Requests

No stipulation.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of The Modified Certificate by the CA

No stipulation.

4.8.7. Notification of Certificate Issuance by The CA to Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

- Suspecting confidentiality of its private key,

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

- Modification in the information contained in the certificate,
- Termination of domain name ownership,
- Mis-issuance of the certificate.

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

- The Subscriber requests in writing without specifying a reason that the Kamu SM revoke the certificate (CRLReason: “unspecified (0)”),
- Kamu SM is informed by the organization or it is determined that the Applicant Representative is not legally authorized to submit the SSL Application (CRLReason #9, privilegeWithdrawn),
- Kamu SM obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise (CRLReason #1, keyCompromise),
- Kamu SM is made aware of a demonstrated or proven method that can easily compute the Subscriber’s Private Key based on the Public Key in the Certificate (such as a Debian Weak Keys, see Section 6.1.1) (CRLReason #1, keyCompromise),
- Kamu SM obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name the certificate should not be relied upon (CRLReason #4, superseded).

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

- Determining the certificate was not issued in accordance with CA/B Forum Baseline Requirements or CP/CPS (CRLReason #4, superseded),
- The emergence of forgery or inaccuracy of the information of the Subscriber in the certificate (CRLReason #9, privilegeWithdrawn),
- The emergence of modification in the information contained in the certificate (CRLReason #9, privilegeWithdrawn),
- Determining use of the certificate in contradiction with the requirements set forth in SSL Certificate Application Form and Subscriber Agreement and CP/CPS document (CRLReason #9, privilegeWithdrawn),
- Obtaining evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn),
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn),
- Issuing a notification to Kamu SM indicating that a court or an authority has revoked domain name ownership or use the authority of the Subscriber, or this case is identified by Kamu SM (CRLReason #5, cessationOfOperation),
- Key size or cryptographic algorithms used in the issuance of SSL certificate becoming deprecated (CRLReason #4, superseded),
- Obtaining evidence that the method to produce the private key of certificate is wrong/flawed (CRLReason #1, keyCompromise),
- Ceasing the operation of Kamu SM and certificate management operation cannot be continued by other CAs (CRLReason: "unspecified (0)").

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

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

- Determining use of the certificate in contradiction with the requirements set forth in CA/B Forum Baseline Requirements, CP/CPS document,
- Compromise of the private key used by Kamu SM for signing the certificate,
- Key size or cryptographic algorithms used in the issuance of SSL certificate becoming deprecated,
- The emergence of inaccuracy of the information in the certificate,
- Ceasing the operation of Kamu SM and certificate management operation cannot be continued by other CAs.

4.9.2. Who Can Request Revocation

The Subscriber or Kamu SM can initiate revocation under the circumstances provided in Section 4.9.1.1. In case Kamu SM revokes the certificate, Subscriber is informed about revocation.

Only authorized revocation requests received from either the Subscriber or the Applicant Representative shall be accepted.

Additionally, relying parties, application software suppliers or any other third parties may submit certificate problem reports as stated in Section 4.9.5 to notify Kamu SM of reasonable cause to revoke the certificate.

4.9.3. Procedure for Revocation Request

SSL certificate revocation application shall be made by the Applicant Representative with the “SSL Certificate Revocation Form” that is available on Kamu SM web site. The Applicant Representative should send the scanned version of the signed and sealed/stamped form from his corporate e-mail address to ssliptal@kamusm.gov.tr e-mail address designated for revocation requests published in the Kamu SM web site. Kamu SM contacts with the Subscriber over the phone call to confirm the revocation request. If the request is confirmed, Kamu SM shall revoke the certificate and update the certificate revocation status.

If the revocation request cannot be confirmed within 24 hours, Subscriber is informed that the revocation process cannot be completed.

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

In case of revocation of root or subordinate CA certificates of Kamu SM, revocation status shall be announced to relevant parties as soon as possible. All certificates issued by root or subordinate CA shall be revoked. The “CRLReason/ReasonCode” revocation code containing the appropriate revocation reason is added to the CRL file and/or OCSP responses that are used for revocation control of the subordinate CA certificate. After revocation, Subscribers shall be duly notified via e-mail or SMS.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.9.4. Revocation Request Grace Period

Revocation request grace period means that the maximum time that the Subscriber may delay the certificate revocation request. The Subscriber should communicate its revocation request to Kamu SM as soon as possible. Kamu SM shall not be held responsible for the issues of the Subscriber arising from the delay of revocation request.

4.9.5. Time within which CA Must Process the Revocation Request

Kamu SM revokes the certificate within 24 hours by making the necessary verifications after receiving the revocation request. If the revocation request cannot be confirmed, the status of the certificate is not changed. This revocation information will be reflected to the OCSP server immediately and a new CRL shall be published within 24 hours after recording a certificate as revoked. If there is an inconsistency in the certificate revocation status between the revocation control mechanisms, OCSP response should be considered. Revoked certificates cannot be reinstated.

If there is a problem detected in the SSL certificate by the third party, an investigation request may be submitted to Kamu SM by sending an e-mail to the problem reporting address specified in Section 1.5.2. In the next 24 hours, Kamu SM does investigate the SSL certificate and provide a preliminary information on its findings to both the Subscriber and the third party who request the investigation. Kamu SM decides the revocation status of the certificate in accordance with the Section 4.9.1.1 and informs the Subscriber and the third party about the certificate status.

Kamu SM maintain continuous 24x7 ability to accept and respond to revocation requests and certificate problem reports.

4.9.6. Revocation Checking Requirement for Relying Parties

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

Prior to relying upon a certificate, relying parties should validate and check the revocation status of all certificates using CRL or OCSP. If technical facilities are eligible, performing certificate revocation check over OCSP is the method recommended by Kamu SM.

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

4.9.7. CRL Issuance Frequency

Kamu SM update and publish a new CRL which contains revocation information of Subscriber certificates at least once a day. The validity period of this CRL is 36 hours at most. The new CRL is published before the time specified in the *nextUpdate* field in CRL.

Kamu SM update and publish a new CRL which contains revocation information of subordinate CA certificate at least once a year. The validity period of this CRL is 1 (one) year at most. If a subordinate CA certificate is revoked, a new CRL shall be published immediately after recording the certificate as revoked. CRL files published by Kamu SM shall be archived.

Kamu SM shall continue issuing CRLs until Subordinate CA Certificate is expired or revoked; or the corresponding Subordinate CA Private Key is destroyed.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.9.8. Maximum Latency for CRLs

CRLs are posted to the repository within the shortest time possible after generation.

4.9.9. Online Revocation/Status Checking Availability

Kamu SM OCSP servers support requests and responses over HTTP in accordance with RFC 6960 [X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)]. Kamu SM OCSP servers can respond to GET and POST requests made by Subscribers.

When a revocation query is issued for a certificate serial number that does not exist in the Kamu SM system, the OCSP server returns an "UNKNOWN" as a response.

The validity period of OCSP responses does not exceed 16 hours. For each OCSP request, an up to date OCSP response is provided.

Kamu SM provides OCSP services and responses for all certificates presumed to exist based on the presence of a precertificate [RFC 6962], even if the final certificate does not actually exist. OCSP server starts to provide authorized responses for the precertificates within 15 minutes after their signing.

4.9.10. Online Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

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

4.9.12. Special Requirements Related to Key Compromise

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

In cases where Kamu SM discovers or has reasons to believe compromise of Subscriber’s key, it shall revoke the certificate and notify the Subscriber.

Third parties may request the revocation of an SSL certificate issued by Kamu SM on the grounds that the private key has been compromised. In this case, in order to prove that the private key has been compromised, the certificate request file (CSR) with the statement that the key has been compromised in the "Common Name" field should be created with the relevant private key and sent by e-mail to the address specified in Section 4.9.3.

Kamu SM may allow additional, alternative methods that do not appear in this section at its own discretion.

4.9.13. Circumstances for Suspension

Certificate suspension is not supported for SSL certificates.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

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

4.10.1. Operational Characteristics

Kamu SM provides a certificate status service either in the form of a CRL or OCSP or both in the certificates. CRL file can be accessible from “CRL Distribution Point” field of the certificate. OCSP responder address is stated in the “Authority Information Access” field of the certificate. Access address of OCSP service is also provided in Section 4.9.9 and CRL files are published in the repository.

Revoked certificates will not be removed from the CRL and OCSP before their expiration dates.

4.10.2. Service Availability

Kamu SM shall take all required measures for providing CRL and OCSP services uninterruptedly on a 24/7 basis.

Kamu SM operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

4.10.3. Optional Features

No stipulation.

4.11. END OF SUBSCRIPTION

Subscriber’s subscription shall terminate when the certificate expires, is revoked or Kamu SM terminates certification services. In cases where Kamu SM terminates certification services or the certificate is revoked, Kamu SM shall notify the Subscriber and/or the Applicant Representative. In case of expiration, Kamu SM shall not have to notify the Subscriber; the Subscriber shall be liable for following the expiration time of its certificate by its own.

4.12. KEY ESCROW AND RECOVERY

Since Kamu SM does not generate the key pair on behalf of Subscribers, Kamu SM may not reissue or backup the keys of the Subscribers.

4.12.1. Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Kamu SM's certificate management process includes:

- Physical security and environmental controls
- System integrity controls (configuration management, malware detection/prevention etc.)
- Network security and firewall management (port restrictions, IP address filtering etc.)
- User management, separate trusted-role assignments, education, awareness, and training
- Logical access controls, activity logging, and inactivity time-outs to provide individual accountability

Kamu SM carries out a risk assessment to evaluate the risks related to certification management process. Kamu SM's risk assessment identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes. Kamu SM assesses the likelihood and potential damage of these threats. The sufficiency of the policies, procedures, information systems, technology, and other arrangements that Kamu SM has in place to counter such threats are also assessed.

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

Kamu SM Information Security Policy that has been approved by management is available on the Kamu SM website.

System configurations are regularly checked to detect data breaches in accordance with the information security policy and related procedures of Kamu SM.

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

5.1. PHYSICAL SECURITY CONTROLS

Kamu SM maintains physical and environmental security policies for systems used for certificate issuance and management process.

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

Private keys of the Kamu SM's CAs are physically separated from the area where normal operations take place. At least 2 (two) authorized personnel must be present at the same time to access this area.

5.1.1. Site Location and Construction

Kamu SM operations are conducted within facilities in Gebze and Ankara. Gebze facility is located away from the city where the disasters such as fire, flood, earthquake, lightning and air pollution have minimal impact. Access to areas and the buildings are protected by multiple tiers of physical security, video monitoring and authentication. Ankara facility is a metropolitan area with levels of physical access controls.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

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

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

5.1.2. Physical Access

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

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

5.1.3. Power and Air Conditioning

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

- Power supply units
- Distribution panels
- Transformer
- UPS devices
- Dry accumulator
- Emergency power generator

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

5.1.4. Water Exposures

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

5.1.5. Fire Prevention and Protection

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

5.1.6. Media Storage

All data storage media are protected physically and electronically against corruption, aging and accidental damage. In addition, on-site backups of the media deemed necessary are taken, as well as backups in a geographically separate location that meets the necessary security criteria.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.1.7. Waste Disposal

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

5.1.8. Off-Site Backup

Kamu SM has a geographically separate, remote disaster recovery center for backup in different locations. Kamu SM stores the components deem necessary in secure safes in a different physical location to ensure the continuity of the system. The locations, where the backups are located, meets all the security and functionality requirements of the main system. Only authorized personnel have access to backup servers and environments.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Roles of personnel employed in Kamu SM have been identified in accordance with ETSI EN 319 401 standard and have been classified as follows:

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

Security Officer: Security Personnel is responsible for administering the implementation of the Kamu SM's security practices.

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

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

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

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

Certificate Issuance Personnel: Certificate Issuance Personnel is responsible for the verification of domain authorization and the CSR file, creation of CA key pair and also issuance of the certificates.

Validation Specialists: Personnel who performs the information verification duties specified by this CP/CPS document within the scope of the CA/B Forum Baseline Requirements. In Kamu SM procedures, Certificate Enrolment Personnel and Certificate Issuance Personnel work as Validation Specialist.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.2.2. Number of Persons Required per Task

Kamu SM requires presence of at least 2 (two) authorized personnel at the same time for issuing and revoking CA certificates.

Kamu SM requires presence of at least 2 (two) authorized personnel at the same time for back up, storage, and recovery of CA private key in a physically secured environment.

5.2.3. Identification and Authentication for Each Role

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

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

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

5.2.4. Roles Requiring Separation of Duties

Separation of duties exist among;

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

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the certificate management process, Kamu SM verifies the identity and trustworthiness of such person. Kamu SM employs personnel that possess the expert knowledge, experience, and qualifications necessary for the offered services, as appropriate to the job function.

5.3.2. Background Check Procedures

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

5.3.3. Training Requirements

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

Kamu SM provides training to its employees at least once a year to raise awareness about information security policies, cybersecurity, and social engineering attacks. In addition, Validation Specialist are trained within the scope of their duties in certificate management processes.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.3.4. Retraining Frequency and Requirements

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

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

In the event that Kamu SM employee create completely or partially fake electronic certificates, forges or falsifies validly created electronic certificates, create electronic certificates without authorization or knowingly uses these electronic certificates, and in the other unauthorized actions, legal investigation and disciplinary process are initiated in accordance with the relevant legislation, depending on the type of violation of information security policies and the extent of the violation.

5.3.7. Independent Contractor Controls

Personnel in trusted roles cannot be independent contractors. There are no Delegated Third Party's personnel involved in the issuance of a certificate.

5.3.8. Documentation Supplied to Personnel

Kamu SM provides its personnel technical and operational documents such as policies or procedures in relation to their job responsibilities.

5.4. AUDIT LOGGING PROCEDURES

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

5.4.1. Types of Events Recorded

Kamu SM records at least the following events:

- CA certificate and key lifecycle events
  - Key generation, backup, destruction
  - Certificate request, issuance and revocation
  - Cryptographic device lifecycle management events
  - Generation of certificate revocation lists
  - Signing of OCSP responses
  - Introduction of new certificate profiles and retirement of existing certificate profiles
- Subscriber certificate lifecycle management events
  - Certificate requests, issuance and revocation
  - All verification activities stipulated in the Kamu SM CP/CPS and CA/B Forum BRs
    - Information being validated (e.g., FQDN or the organization name)

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

        - Authorization Domain Name (ADN) used (if applicable and different from the applied-for FQDN)
        - Validation method used (e.g., the BRs section number)
    - Approval and rejection of certificate requests
    - Generation of certificate revocation lists
    - Signing of OCSP responses
    - Records of the unique identifier of each Network Perspective used for Multi-Perspective Issuance Corroboration, the attempted domain name, and the result of the validation attempt
    - Multi-Perspective Issuance Corroboration quorum results for each attempted domain name
    - Forms or documents taken electronically or manually during application
- Other events related to security
    - System start-up and shutdown
    - Successful and unsuccessful PKI system access attempts
    - Security system actions performed by personnel
    - Security sensitive files or records read, written or deleted
    - Security profile changes
    - Installation, update and removal of software on a certificate system
    - System crashes, hardware failures, and other anomalies
    - Firewall and router activities
        - Successful and unsuccessful login attempts to routers and firewalls
        - All administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications
        - All changes made to firewall rules, including additions, modifications, and deletions
        - All system events and errors, including hardware failures, software crashes, and system restarts
    - Entries to and exits from Kamu SM CA facility

Log records include description of event, date/time of event and identity of the person making the journal record.

5.4.2. Frequency of Processing Log

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

Electronic or manual records of information received from Subscribers during certificate application process may be reviewed as necessary during the certificate lifecycle or for legal purposes.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.4.3. Retention Period for Audit Log

Kamu SM retains following audit logs for at least 2 (two) years, or as long as they are required to be retained per laws and/or ETSI standards, whichever is longer:

- CA certificate and key lifecycle management event records after the later occurrence of the destruction of the CA Private Key; or the revocation or expiration of the CA Certificate.
- Subscriber certificate lifecycle management event records after the expiration of the Subscriber certificate.
- Any security event records after the event occurred.

5.4.4. Protection of Audit Log

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

- Unauthorized people may not access the systems where electronic audit logs are stored.
- Manual audit logs are stored in locked rooms and can be accessed only by the authorized personnel.
- The records shall not be deleted, altered or destroyed within the required legal period. In this direction, necessary security measures are taken.
- Audit logs posing criticality in terms of system operation are signed digitally and stored. In this way, all kinds of modifications likely to occur in critical records will be noticed by the system.
- Critical information is stored encrypted with keys of Kamu SM, when necessary.

5.4.5. Audit Log Backup Procedures

Considering criticality of the system, online backups of necessary logs are taken regularly on a daily basis when the system is not intensively used. There is a tape library to meet backup needs and backup management software to automate backup operations. Critical audit logs are backed up in secure disaster recovery facilities located in geographically separate city.

5.4.6. Audit Collection System (internal vs. external)

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

5.4.7. Notification to Event-Causing Subject

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

5.4.8. Vulnerability Assessments

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

Details on the assessment of vulnerabilities are defined in Kamu SM's Vulnerability Management Policy. In accordance with this internal policy document, Kamu SM performs regular vulnerability scanning and penetration testing. Recorded vulnerabilities are processed based on risk assessment events.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

In addition to the logs specified in Section 5.4.1, the following electronic or manual documents in relation to certificate application and certificate life cycle are archived:

- All information and documents provided during application by the Subscriber and records of their verification
- Forms received electronically or manually during certificate issuance and revocation applications
- All issued certificates
- All expired Kamu SM root and subordinate CA certificates
- All published certificate revocation status logs
- Certificate Policy and Certification Practice Statement document
- Certificate management procedures
- Subscriber agreements
- NTP synchronization logs of systems that used for certification processes

Kamu SM archives documentation related to the security of certificate systems, certificate management systems and root CA systems.

5.5.2. Retention Period for Archive

Archived audit logs as set forth in Section 5.5.1 are retained for a period of minimum 2 (two) years from their record creation timestamp, or as long as they are required to be retained per laws and/or ETSI standards, whichever is longer.

5.5.3. Protection of Archive

Archived data and documents are retained electronically and physically secure environments to prevent unauthorized monitoring, modification, and deletion. Only authorized personnel have access to archives. The environment in which the archives are retained is selected in a way that will prevent damaging of archives during time frame set out in Section 5.5.2.

5.5.4. Archive Backup Procedures

Electronic archives containing critical information are backed up in pursuance of Kamu SM Business Continuity Policy.

5.5.5. Requirements for Time-Stamping of Records

Kamu SM adds time stamping to records where it deems necessary. Irrespective of timestamping methods, all logs have data indicating the time at which the event occurred.

5.5.6. Archive Collection System (Internal or External)

Archives are collected according to relevant Kamu SM procedures either in electronic or paper form.

5.5.7. Procedures to Obtain and Verify Archive Information

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.6. KEY CHANGEOVER

Keys and certificates of Kamu SM may be renewed due to expiry, security concerns or changes in certificate profiles. Prior to the expiration of the certificate of Kamu SM, key changeover procedures are done. Key changeover process requires the following:

- Certificate issuance with the old key is ceased.
- Old Kamu SM certificate continues to be published in order for certificates to be verified which are signed with old Kamu SM private key.
- If CRL file and certificates are signed with the same private key, Kamu SM continues to sign CRLs with the same private key until the last expiration date of the certificates issued using this private key. CRL file created for newly issued certificates is signed with new Kamu SM private key.
- Renewed Kamu SM CA certificates are made available through the Kamu SM repository.
- Renewed Kamu SM CA certificates are disclosed to the CCADB within the period specified in Root Programs and/or the BRs.

5.7. COMPROMISE AND DISASTER RECOVERY

Information systems monitored for possible security violations and detected violations are reported. Any critical vulnerability not previously addressed by the Kamu SM is addressed within a period of 48 hours after its discovery. Start-up and shutdown of the logging functions, availability, and utilization of needed services are monitored.

5.7.1. Incident and Compromise Handling Procedures

In case of a compromise, (incident or security vulnerability etc.) the processes in the Kamu SM's internal procedures are carried out to ensure that the certificate management system starts to operate reliably again within the shortest time possible, that the affected parties and its damages are minimized. If any, affected parties are informed within 24 hours.

Business Continuity Plans have been prepared in order to draw a response and management framework for events that may interrupt operations in the event of a disaster, security compromise or business failure within Kamu SM. These plans are tested, reviewed and updated on at least annual basis.

Kamu SM maintains a plan for mass revocation events, conducts annual testing of the plan and updates it as necessary based on insight gained from these tests. This process is carried out in combined with the Business Continuity Plans.

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

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

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

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

5.7.3. Entity Private Key Compromise Procedures

If it is suspected or learned that the confidentiality of the private key used by Kamu SM for certificate signing has been lost, the relevant certificate is revoked within the shortest time possible and following actions are taken within the business continuity plans:

- Kamu SM announces the revocation of the certificate together with the reason for revocation as soon as possible via https://kamusm.bilgem.tubitak.gov.tr website and notifies all affected parties in writing.
- Revoked Kamu SM CA certificates are disclosed to the CCADB within the period specified in Root Programs and/or the BRs.
- Kamu SM makes a statement indicating how the Subscribers will be affected and issues a notice to affected parties not to rely on the certificates signed with old private keys.
- Kamu SM states revoked status of its certificate in CRL file.
- Some or all of the certificates issued by Kamu SM are revoked when deemed necessary. Subscribers are notified of certificate's revoked status within the shortest time possible.
- Kamu SM ceases to respond to new certificate requests.
- Interested parties are notified in the ongoing basis in relation to the status of Kamu SM.
- Kamu SM processes destruction of the private key.
- Kamu SM delivers a new certificate to the parties by generating a new key pair and issuing a certificate.
- Upon renewal of key pair of Kamu SM, the process of issuing new certificates instead of revoked ones is initiated in line with the requests received from the users.

5.7.4. Business Continuity Capabilities after a Disaster

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

Kamu SM maintains a disaster recovery facility located at another city. Kamu SM takes backups of important data and applications in accordance with Backup Management Policy which identify important data, time period and personnel roles and when necessary, recovery procedure is applied. In order to maintain business continuity, backups of data stored in Kamu SM head office are also retained in disaster recovery center.

Kamu SM periodically revises and tests Kamu SM Business Continuity Plans that will ensure restoration and recovery after a failure. Kamu SM takes necessary measures to prevent the recurrence of failure situations.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

5.8. CA OR RA TERMINATION

In the event that Kamu SM terminates its CA services, the termination process shall be carried out in accordance with the Kamu SM Certification Services Termination Plan and applicable legislation.

The plan defines the procedures for:

- Notifying subscribers, relying parties, and relevant authorities,
- Discontinuing certificate issuance,
- Managing the revocation status of certificates,
- Ensuring continuity of CRL and OCSP services,
- Secure destruction or transfer of private keys,
- Retention of records and archives.

Where CA services are transferred to another CA, such transfer shall be performed in accordance with the Kamu SM Certification Services Termination Plan and applicable standards.

6. TECHNICAL SECURITY CONTROLS

The systems that Kamu SM generates its own key pairs and the activation data and performs all certificates management operations all conform to ETSI EN 319 401, ETSI EN 319 411-1 and CA/B Forum the BRs.

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

Key pairs of roots and subordinate CAs shall be generated by the personnel in trusted roles under the principles of multiple person control and split knowledge, by using secure software and/or hardware meeting FIPS PUB 140-2 Level 3 or EAL4+ standards, passed from the testing required for secure key generation, in closed network environment and in a secure room where unauthorized personnel cannot access. Generated private keys shall be stored within the secure cryptographic module. The module cannot be moved out of the secure room. All procedures conducted shall be recorded and shall be approved by the personnel having performed the procedure.

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

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

Key pair generation for SSL certificates shall be performed by the Subscriber. Kamu SM shall not generate a key pair on behalf of a Subscriber and shall reject the certificate request if one or more of the following conditions are met:

- The key pair does not meet the requirements defined in Section 6.1.5 and/or Section 6.1.6,
- There is clear evidence that the specific method used to generate the private key was flawed,
- Kamu SM is aware of a demonstrated or proven method that exposes the Applicant’s private key to compromise,
- Kamu SM has previously been made aware that the Applicant’s private key has suffered a key compromise,

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

- Kamu SM is aware of a demonstrated or proven method to easily compute the Applicant's private key based on the public key
    - Debian Weak Keys, ROCA Vulnerability, RSA Close Primes (Fermat Attack), etc.

6.1.2. Private Key Delivery to Subscriber

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

6.1.3. Public Key Delivery to Certificate Issuer

SSL certificate Applicant shall deliver its public key in PKCS#10 format to Kamu SM via e-mail by using its corporate e-mail in the certificate application process.

6.1.4. CA Public Key Delivery to Relying Parties

Root, subordinate CA and cross certificates (if any) shall be made available for access of the relying parties through the Kamu SM repository.

6.1.5. Key Sizes

For SSL certificate RSA key pairs Kamu SM ensures that:

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

For SSL certificate ECDSA key pairs Kamu SM ensures that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

No other algorithms or key sizes are permitted.

6.1.6. Public Key Parameters Generation and Quality Checking

Kamu SM performs key generation and quality checking in accordance with the requirements specified in Section 6.1.6 of the BRs. Both RSA and ECDSA key pairs are supported.

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

The permitted usage purposes of the keys issued by Kamu SM are specified in the "Key Usage" and/or "Extended Key Usage" extensions included in the certificates.

The private key corresponding to Kamu SM Root Certificate is used to sign subordinate CA certificates, cross certificates and CRLs. OCSP responses are signed using OCSP certificates delegated by root and/or subordinate CAs. Private keys corresponding to Root Certificates are not used to sign certificates except as permitted by section 6.1.7 of the BRs.

Kamu SM may issue multiple CA certificates containing the same public key. This may occur in the context of cross-certification or transition processes where CA certificates signed by different issuers exist for the same key pair.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

The cryptographic module has the following security functions specified:

- It provides confidentiality and integrity throughout the validity period of the private key.
- It meets identification and authentication functions in accessing the module.
- It can be defined in a manner that access authority shall be under the control of several authorized personnel.
- It restricts access to the services offered in line with the roles defined for the user.
- All kinds of physical measures likely to lead to tampering with use and unauthorized access to the module have been properly taken.
- In case of attempting unauthorized access, the module shall delete the data inside it.
- It enables secure backup of the private key.
- The cryptographic module shall meet a minimum one of the following security standards: FIPS PUB 140-2 Level 3 (or higher) or EAL 4 (or higher) in accordance with ISO/IEC 15408.
- Cryptographic modules that have retired and/or malfunctioned cannot be taken out of the secure area and destroyed in accordance with the destruction procedure.

6.2.2. Private Key Multi-Person Control

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

6.2.3. Private Key Escrow

Not applicable.

6.2.4. Private Key Backup

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

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

6.2.5. Private Key Archival

Kamu SM does not archive private keys.

6.2.6. Private Key Transfer into or From a Cryptographic Module

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

6.2.7. Private Key Storage on Cryptographic Module

Kamu SM private keys are kept in encrypted form with secure algorithm and methods within secure cryptographic hardware device having FIPS PUB 140-2 Level 3 or EAL4+ certificate, as blocked to access of unauthorized people. Transfer of private keys outside of the device has been blocked except for the backup purpose.

6.2.8. Method of Activating Private Keys

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

While private key is in the encrypted state within the cryptographic module, it is not in active state. Required data should be provided to the module for activation. Kamu SM private keys are activated in accordance with the instructions and documentation provided by manufacturer of the hardware security module.

6.2.9. Method of Deactivating Private Keys

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

6.2.10. Method of Destroying Private Keys

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

6.2.11. Cryptographic Module Rating

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

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Usage period of private keys is as usage period of the certificate. Usage of private keys expires upon expiration of the certificate or revocation of the certificate. Subscriber certificates must not have a validity period greater than 200 days. The validity period of Subscriber certificate cannot exceed the validity period of Kamu SM certificate.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

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

Activation data are generated in compliance with the characteristics of the cryptographic module. Cryptographic modules used by Kamu SM minimum conform to FIPS PUB 140-2 Level 3 or EAL4+.

6.4.2. Activation Data Protection

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

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

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

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

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

Controls are provided below while performing system development:

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

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

6.6.2. Security Management Controls

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

6.6.3. Life Cycle Security Controls

No stipulation.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

6.7. NETWORK SECURITY CONTROLS

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

Network and system management and security agents are deployed on the servers. Management software retrieves the information such as a disk, memory, processor usage, file integrity, security log entries, external storage unit tracks etc. and monitor this information in real time. Threshold values are identified for sources that are of importance for the operation of servers and in case these threshold values are exceeded, the system administrator is automatically alerted. Network and system management and security infrastructure store such retrieved information in a central database. In this way, it enables to query data at any time and to issue past reports. If Kamu SM needs to communicate distinct trustworthy systems, Kamu SM establishes trusted channels which are logically distinct from other communication channels.

Different network segments have been issued for the high-security systems (such as root and subordinate CA servers). Root servers are kept turned off. These servers are turned on only, when necessary, states defined in Kamu SM's system, network and access procedures, and are turned off again when the processes are completed. Kamu SM's production systems for its services are separated from testing and development systems. Accessing secure zones and high secure zones are granted in accordance with the access control policy. Hardware that are used in high-security systems are not re-used in different places and they are destroyed.

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

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

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

6.8. TIME-STAMPING

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

7. CERTIFICATE, CRL AND OCSP PROFILES

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

7.1. CERTIFICATE PROFILE

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

Precertificates, submitted to Certificate Transparency logs and containing the critical poison extension (OID: 1.3.6.1.4.1.11129.2.4.3), are issued directly by the subordinate CA in accordance with the profile specified in CA/B Forum Baseline Requirements.

Certificate *serialNumber* is a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from CSPRNG. As an exception to RFC 5280, the SSL precertificate and the final SSL certificate have the same *serialNumber* value.

The contents of the SSL certificates issued by Kamu SM are provided in Appendix-A. The use of cross-certification does not introduce any changes to the profiles of SSL certificates issued under this CPS.

7.1.1. Version Number(s)

Kamu SM issues certificates in compliance with X.509 v3.

7.1.2. Certificate Content and Extensions

Certificates issued by Kamu SM include X.509 v3 certificate extensions and mandatory fields in accordance with IETF RFC 5280.

SSL certificates include the Extended Key Usage extension and assert only the *id-kp-serverAuth* purpose.

SSL certificates include the Subject Alternative Name extension populated in accordance with RFC 5280 and contain the validated domain name specified in the *commonName* attribute of the Subject Distinguished Name (DN). This extension may also contain additional validated domain names.

SSL certificates include the Signed Certificate Timestamp List extension in accordance with the Certificate Transparency requirements.

Subordinate CA and cross certificates newly issued by Kamu SM serve a single trust purpose and include the Extended Key Usage extension asserting only the *id-kp-serverAuth* purpose.

All certificates issued within the Kamu SM SSL hierarchy are created in accordance with the certificate profiles defined in the BRs.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

7.1.3. Algorithm Object Identifiers

Kamu SM uses signature algorithms and encodings in line with Section 7.1.3 of the BRs. The algorithm that may be used are listed in the table below.

Algorithm	OID
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
sha384WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12]
sha512WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13]
ecdsa-with-SHA256	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2]
ecdsa-with-SHA384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3]
ecdsa-with-SHA512	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4]

Certificates, CRLs, and OCSP responses issued by Kamu SM may be signed using RSA or ECDSA signature algorithms together SHA-256 or stronger hash functions, depending on the key type of the issuing CA.

7.1.4. Name Forms

Kamu SM issues certificates with name forms compliant with RFC 5280 and Section 7.1.4 of the BRs.

Attributes that appear within the *Subject* field of the SSL certificate are *countryName*, *stateOrProvinceName*, *organizationName* and *commonName* respectively. The content of each attibute is defined in Section 3.1.5.

Kamu SM does not issue SSL certificates for IP Addresses or internal server names.

7.1.5. Name Constraints

Kamu SM provides OV SSL services to organizations using domain names ending with ".tr" ccTLD. SSL certificates are not issued for domain names under other ccTLDs.

7.1.6. Certificate Policy Object Identifier

The Certificate Policies extension of SSL certificates issued by Kamu SM includes the following policy identifiers:

- CA/B Forum Organization Validated OID (2.23.140.1.2.2)
- Kamu SM OV SSL OID (2.16.792.1.2.1.1.5.7.1.3)

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

Policy qualifiers are not used in the Certificate Policies extension of certificates issued by Kamu SM.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

7.2. CRL PROFILE

Kamu SM issues CRL in compliance with the document of "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" and in accordance with the profile specified in CA/B Forum Baseline Requirements.

CRLs published by Kamu SM contain as a basis the issuer information, CRL number, issue date of CRL, date on which next CRL will be published, and serial numbers and revocation dates of revoked certificates. Kamu SM does not issue partitioned (sharded) CRLs. Each published CRL is a full and complete CRL containing information on all revoked and unexpired certificates.

7.2.1. Version Number(s)

Kamu SM issues version 2 CRLs in compliance with RFC 5280.

7.2.2. CRL and CRL Entry Extensions

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

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

*Reason codes used for revocation of SSL certificates issued by Kamu SM are listed below in order of priority:

1. RFC 5280 CRLReason #1: keyCompromise
2. RFC 5280 CRLReason #9: privilegeWithdrawn
3. RFC 5280 CRLReason #5: cessationOfOperation
4. RFC 5280 CRLReason #3: affiliationChanged
5. RFC 5280 CRLReason #4: superseded

Subscriber should request revocation of their certificates by selecting one of the revocation reasons specified in the "SSL Certificate Revocation Form". If the situation is that multiple revocation reasons apply, the revocation reason of higher priority should be selected. In case SSL certificates are revoked for one of the reasons below, Kamu SM includes the specified *CRLReason* in the *ReasonCode* extension of the CRL entry corresponding to the SSL certificate. Permitted revocation reasons and the explanation about when to choose each option are given below:

- **Private Key is Stolen/Lost** (keyCompromise): The Subscriber must choose this option when loss or deletion of the private key corresponding to the public key in the certificate or if it is understood that private key has been compromised by unauthorized person.
- **Termination of Domain Name Ownership/End of Domain Name Usage** (cessationOfOperation): The Subscriber should choose this option when the ownership of the certified domain name expires or the website containing the relevant domain is no longer be used prior to the expiration of the Certificate.
- **Changes in the Certificate's Subject Information** (affilationChanged): The Subscriber should choose this option when there is a change in the information (Organization, StateorProvince, etc.) given during the certificate application and written on the content of the certificate.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

- **Certificate Misissuance** (superseded): The Subscriber should choose this option when a mistake is noticed in the validity date, issuer and subject fields of the certificate or in the certificate structure.
- **New Certificate Request** (superseded): The Subscriber should choose this option when the Subscriber requested new certificate to replace an existing certificate.
- **Other** (RFC 5280 CRLReason #0: unspecified): It should only be selected if any of the above-mentioned revocation reasons are not suitable.

The "*privilegeWithdrawn*" reason code is used in case the Subscriber provides misleading information in the certificate application or failing to fulfil its important obligations under the Subscriber agreement or terms and conditions. Since the use of this revocation reason is determined by the Kamu SM, it is not presented to the Subscriber as a reason for revocation. When the certificate is revoked due to this revocation reason, "*CRLReason/ReasonCode*" extension is added to the CRL entry corresponding to the certificate in the CRL file.

The "*Other*" revocation reason is presented to the user as the default option in cases where one of the specified revocation reasons is not applicable. If the Subscriber chooses the "*Other*" revocation reason, no "*CRLReason/ReasonCode*" extension is provided in the CRL entry corresponding to the certificate in the CRL file.

In case subordinate CA certificates of Kamu SM are revoked, the appropriate "*CRLReason/ReasonCode*" extension is added to CRL entry corresponding to the certificate in the CRL file.

7.3. OCSP PROFILE

Kamu SM provides OCSP service in compliance with the document of "IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP". Kamu SM OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the certificate whose revocation status is being checked.

Kamu SM issues OCSP Responder Certificates in accordance with the profile specified in CA/B Forum Baseline Requirements. OCSP Responder Certificates contain an extension of type *id-pkix-ocsp-nocheck*, as defined by RFC 6960.

In case of providing OCSP service*, revocationReason* field is present for OCSP responses for subordinate CA certificates, if the certificates are revoked. The *CRLReason* indicated contains a value permitted for CRLS, as specified in Section 7.2.2.

7.3.1. Version Number(s)

Kamu SM issues version 1 OCSP responses in compliance with RFC 6960.

7.3.2. OCSP Extensions

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

The *singleExtensions* of an OCSP response does not contain the *reasonCode* CRL entry extension.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies and procedures within this CP/CPS are designed to comply with the requirements of generally accepted industry standards, including the latest versions of ETSI EN 319 411-1 and CA/B Forum the BRs and other programs listed in Section 1.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Audits within the scope of ETSI EN 319 411-1 and CA/B Forum the BRs are made by a qualified auditor on an annual and contiguous basis. An audit period does not exceed one year in duration and the scope of these audits is limited to OV SSL.

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

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor is selected from the qualified auditors accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403. Additionally, qualified auditors shall meet the criteria specified in the Root Programs and the BRs.

Assessors are competent people in the issue of the audit of public key infrastructure technology, information security and technology, and information systems. Assessors conduct their audits independently.

ISO 27001 lead-auditor certificate is needed for ISO 27001 audits.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

Kamu SM undergoes an audit in accordance with the latest version of the ETSI EN 319 411-1, which include normative references to ETSI EN 319 401.

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

The audit covers;

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

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance, then the auditor will promptly notify Kamu SM and document the deficiency. Kamu SM will identify the actions to be performed for remedying deficiencies under the leadership of Kamu SM management.

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

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

8.6. COMMUNICATION OF RESULTS

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

Audit reports are made publicly available within 3 (three) months after the end of the audit period through Kamu SM website or audit firm's website.

8.7. SELF-AUDITS

Kamu SM checks compliance of SSL certificates with its CP/CPS the BRs by performing self-audits on at least a quarterly basis against a randomly selected samples of at least three percent of the SSL certificates issued since the last self-audit. s

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

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

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

9.1.2. Certificate Access Fees

Kamu SM publishes its own certificates free of charge.

9.1.3. Revocation or Status Information Access Fees

Kamu SM does not charge a certificate revocation fee or a fee for checking the validity status of an issued certificate using CRL or OCSP.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

9.1.4. Fees for Other Services

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

Kamu SM will not charge a fee for access to the information and documents published in the repository.

9.1.5. Refund Policy

If the subscriber determines that it is unable to use its certificate upon initial delivery, within the period specified in CP/CPS Section 4.4.1 and if it is determined that the issue arises from an error resulting from Kamu SM, the fee paid for the certificate shall be refunded upon Subscriber's request.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

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

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

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

Private keys, activation data used to access private keys or to gain access to the CA system, business continuity plans, disaster recovery plans, audit logs and internal Kamu SM business procedure/policy documentation are considered as confidential and protected against disclosure using a reasonable degree of care.

9.3.2. Information Not Within the Scope of Confidential Information

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

9.3.3. Responsibility to Protect Confidential Information

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

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

Kamu SM maintains confidentiality of personal/organizational information of Applicants, Subscribers, and other participants within the scope of the services it provides. All personal data are processed in

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

accordance with applicable data protection legislation, including the law on the Protection of Personal Data No. 6698.

9.4.2. Information Treated as Private

Personal data such as identity information, demographic data, address details and contact information provided to Kamu SM during identification, authentication and certificate lifecycle management processes shall be treated as confidential and processed only for certification service purposes.

9.4.3. Information Not Deemed Private

Information contained in the issued certificates, including but not limited to subject name, domain name, and certificate validity information is considered public and may be disclosed via certificates and related services.

9.4.4. Responsibility to Protect Private Information

Kamu SM collects only the information necessary for certificate issuance and lifecycle management. Such information shall not be used for purposes other than certification services and shall not disclosed to unauthorized third parties, including relying parties, except as permitted by applicable laws or with the explicit consent of the Subscriber.

Kamu SM implements appropriate technical and organizational security measures to protect personal data against unauthorized access, disclosure, alteration, and destruction. Access to such information is restricted to authorized personnel on a need-to-know basis.

Kamu SM provides information as part of Personal Data Protection Law on its website.

9.4.5. Notice and Consent to Use Private Information

Subscribers are informed about data processing activities in accordance with applicable data protection legislation. Where required by law, explicit consent of Subscriber is obtained prior to the processing or disclosure of personal data.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Kamu SM may disclose the private information to competent authorities pursuant to judicial or administrative requests in accordance with applicable laws.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

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

9.6. REPRESENTATIONS AND WARRANTIES

Kamu SM, Subscribers and the relying parties fulfil the representations and warranties mentioned in the agreements.

9.6.1. CA Representations and Warranties

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

- Employ qualified personnel for required by the service,

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

- Execute certification procedures in compliance with policy and practice statements designated thereof,
- Publish CP/CPS document from public access repository,
- Generate key pairs for root and subordinate CAs and issue certificates for these key pairs,
- Publish root and subordinate CA certificates in environments accessible by end users,
- Verify the identity of the Applicant, in accordance with the procedures specified in CP/CPS,
- Verify that the Applicant Representative is authorized to request the certificate on behalf of the Subscriber organization, in accordance with the procedures specified in CP/CPS,
- Verify that the Applicant either had to right to use, or had control of, the domain name(s) listed in the certificate, in accordance with the procedures specified in CP/CPS,
- Ensure the accuracy of all the information contained in the certificates,
- Not issue the certificate for Applicant failed to meet required application requirements,
- Review certificate applications and inform the Applicant regarding the result of the application,
- Accept certificate renewal applications in accordance with the procedures specified in CP/CPS,
- Accept certificate revocation applications in accordance with the procedures specified in CP/CPS and revoke the certificate for any reasons specified in CP/CPS,
- In case it is identified that there is certificate usage not complying with CP/CPS document and the SSL Certificate Application Form and Subscriber Agreement, revoke the relevant certificate,
- Publish revoked certificates information in CRL and announce the same via OCSP service,
- Take required measures to protect the integrity and the accessibility of the active and revoked certificates records uninterruptedly on a 24/7 basis,
- Record all events performed in relation to certificate issuance, management, and revocation,
- Store all hard copy and electronic records securely throughout the periods set forth in CP/CPS.

9.6.2. RA Representations and Warranties

Registration authority representations and warranties are as follows:

- Receive certificate applications,
- Verify the identity information of the Applicant based on the required documents by the methods specified in CP/CPS,
- Receive the required documents and information from the Subscriber,
- Check the CSR,
- Delegate the verified certificate applications to the responsible units of Kamu SM,
- Deliver the SSL certificates to their owners,
- Receive certificate revocation requests,
- Delegate the verified certificate revocation requests to responsible units of Kamu SM,
- Inform the Subscribers about revoked certificates.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

9.6.3. Subscriber Representations and Warranties

Kamu SM requires, as a part of Subscriber Agreement, that the Applicant makes and agrees to the representations and warranties in this section for the benefit of Kamu SM and the certificate beneficiaries.

Prior to the issuance of a certificate, Kamu SM obtains the Applicant's agreement to the Subscriber Agreement with Kamu SM. Subscriber Agreements may include additional representations and warranties.

Subscriber/Applicant representations and warranties are as follows:

- Fulfil the certificate application, revocation, and other procedures in compliance with the principles described in Kamu SM certificate management procedures as set forth in CP/CPS,
- Declare accurate and complete information during certificate application and revocation procedures and as otherwise requested by Kamu SM in connection with the certificate management procedures,
- Check and confirm the accuracy of the information contained in the issued certificate prior to its use,
- Take all reasonable measures to assure control of, keep confidential, and properly protect at all times the private key corresponding to the public key in the certificate,
- If there is any actual or suspected misuse or compromise of the private key, promptly request Kamu SM for revoking the certificate, and immediately cease using the certificate and its associated private key,
- If any information in the certificate is or becomes incorrect or inaccurate, promptly request Kamu SM for revoking the certificate, and cease using the certificate,
- Cease all use of the private key and the certificate upon revocation of that certificate for reasons of key compromise,
- Respond to the Kamu SM's instructions concerning key compromise or certificate misuse within a reasonable time,
- Perform no actions with revoked or expired certificates,
- Install the certificate only on servers that are accessible at the "Subject Alternative Names" listed in the certificate,
- Acknowledge that the SSL certificate shall not be used on servers and systems that cannot tolerate revocation,
- To follow the notification regarding revocation process and act in accordance with the revocation timeline within the periods specified in Section 4.9.1.1 of the Kamu SM SSL CP/CPS document by working in cooperation with the Kamu SM in cases requiring certificate revocation,
- To undertake that the Kamu SM has an obligation to comply with international standards and to accept the decisions and practices taken in the revocation processes,
- Use the certificate solely in compliance with all applicable laws and solely in accordance with Subscriber Agreement and CP/CPS,

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

- Know and accept that Kamu SM is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the CP/CPS or relevant standards.

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

9.6.4. Relying Party Representations and Warranties

Relying parties are responsible for performing appropriate certificate validation checks prior to relying on a certificate. A relying party may be considered to reasonably rely on a certificate only if the following actions are performed:

- Possess the technical capability to process and validate certificates,
- Verify the validity of the certificate, including the certification path,
- Check the revocation status of both the CA and end-entity certificates using CRLs and/or OCSP,
- Ensure that the certificate is used in accordance with its intended purpose,
- Take into account any limitations on certificate usage as specified in the certificate and the applicable CP/CPS,
- Verify that the certificate is within its validity period (not expired).

Any reliance on a certificate without performing the above checks shall be at the relying party's own risk.

9.6.5. Representations and Warranties of Other Participants

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

9.7. DISCLAIMERS OF WARRANTIES

Warranty between Kamu SM and the Subscribers expire as set forth in the SSL Certificate Application Form and Subscriber Agreement.

9.8. LIMITATIONS OF LIABILITY

Kamu SM shall be liable for damages arising from its failure to perform its obligations in accordance with the applicable CP/CPS and the CA/Browser Forum Requirements.

Kamu SM does not guarantee that certificates will be fit for any particular purpose beyond those specified in the applicable CP/CPS.

To the extent permitted by applicable law, Kamu SM shall not be liable for any indirect, incidental, or consequential damages arising from the use of, or reliance on, a certificate.

Kamu SM's liability shall be limited to direct damages that are duly proven in accordance with applicable law.

The liability and/or limitation thereof of Kamu SM, Subscribers, and relying parties shall be further defined in the applicable Subscriber Agreements and related contractual documents.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

9.9. INDEMNITIES

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

9.10. TERM AND TERMINATION

9.10.1. Term

This CP/CPS is effective when published to Kamu SM's online repository and remain in effect until a newer version is published.

9.10.2. Termination

This CP/CPS shall remain in effect until a newer version is published.

9.10.3. Effect of Termination and Survival

Upon termination of this CP/CPS, Subscribers and relying parties are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

Upon expiration of the SSL Certificate Application Form and Subscriber Agreement, liabilities of the organization receiving service relating to ensuring the following requirements in CP/CPS will come to an end.

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

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Kamu SM notifies the Subscriber regarding result of certificate application, revocation and renewal requests. Notices will be made via phone, fax or e-mail. Notifications made to an e-mail of the agency specified in certificate application form, if modified, to a newly notified e-mail address will be considered as official notification.

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

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

Kamu SM reviews its CP/CPS annually and may review more frequently. Amendments likely to be made on the CP/CPS document may be either by way of addition or modification or Kamu SM may decide on the whole renewal of the document. Changes to this CP/CPS are indicated by appropriate numbering. Amendments are made by posting an updated version of the CP/CPS to the online repository of Kamu SM.

Even if it is revealed that any part of the CP/CPS document is inaccurate or invalid, other parts of the CP/CPS document of Kamu SM will survive until the CPS document is updated.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

9.12.2. Notification Mechanism and Period

Amendments made on this CP/CPS document will be announced by way of publicly accessing over repository of Kamu SM. Effective date of CP/CPS is stated in the document. The renewed document is published in the repository within a reasonable time.

9.12.3. Circumstances under Which OID Must Be Changed

No stipulation.

9.13. DISPUTE RESOLUTION PROVISIONS

All disputes arising out of the parties will be settled amicably. It shall be referred to the contracts mutually concluded thereon, agreements, Kamu SM Certificate Policy and Certification Practice Statement in settlement of disputes. Before resorting to any dispute resolution mechanism, parties are required to notify Kamu SM and attempt to resolve disputes directly with Kamu SM. If disputes fail to be settled amicably, competent courts will be Gebze Courts, the Republic of Turkey in settlement of disputes.

9.14. GOVERNING LAW

This CP/CPS is subject to all applicable laws and regulations of Turkish Republic. The laws of the Republic of Turkey shall apply for the implementation and interpretation of the CP/CPS.

9.15. COMPLIANCE WITH APPLICABLE LAW

All related parties including Kamu SM, Subscribers and relying parties agree to comply with applicable laws and regulations as pertaining in Turkish Republic. In the event the provisions contained in CP/CPS document are found to be in contradiction with the relevant legislation to be effective thereafter, required adjustments shall be made and duly adapted.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

Kamu SM requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

If any provision of this CP/CPS is found to be invalid or unenforceable, the remainder of the CP/CPS will remain valid and enforceable.

In the event of a conflict between the BRs and a law, regulation or government order of Turkey, Kamu SM will immediately notify the CA/Browser Forum and will follow the procedures defined in BR Section 9.16.3.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

9.16.5. Force Majeure

To the extent permitted by law, Kamu SM is not be liable for any delay or failure to perform an obligation under this CP/CPS caused by an occurrence beyond its reasonable control.

9.17. OTHER PROVISIONS

No stipulation.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

APPENDIX-A: OV SSL CERTIFICATE PROFILE

Field	Description
Version	V3
Serial Number	A non-sequential positive integer containing at least 64 bits of random output from a CSPRNG.
Signature Algorithm	See Section 7.1.3.
Issuer	Byte-for-byte identical to the Subject field of the issuing Subordinate CA.
Validity Period	See Section 6.3.2.
Subject	Contains validated Subject information. C = TR ST = <StateOrProvince> O = <Organization> CN = <CommonName> (Contains a value derived from the *subjectAlternativeName* extension.)
Subject Public Key	See Section 6.1.5.
Extension	**Description**
Authority Key Identifier	Critical=No; *keyIdentifier* is identical to the *subjectKeyIdentifier* field of the issuing Subordinate CA.
Subject Key Identifier	Critical=No; Contains 160-bit SHA-1 hash of *subjectPublicKey*.
Key Usage	Critical=Yes; Digital Signature (For RSA and ECDSA), Key Encipherment (Only for RSA)
Certificate Policy	Critical=No; CA/B Forum Organization Validated OID (2.23.140.1.2.2) Kamu SM OV SSL OID (2.16.792.1.2.1.1.5.7.1.3)
Extended Key Usage	Critical=No; Server Authentication (1.3.6.1.5.5.7.3.1)
CRL Distribution Points	Critical=No; Contains the HTTP URL of the issuing Subordinate CA's CRL service.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.

Authority Information Access	Critical=No; Contains the HTTP URLs of the issuing Subordinate CA's certificate and OCSP responder.
Subject Alternative Name	Critical=No; Contains at least one *dNSName*.
Signed Certificate Timestamp List	Critical=No; OCTET STRING containing the encoded *SignedCertificateTimestampList*, as specified in RFC 6962.

Notice: No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means without prior written permission of Kamu SM.