MeSign Technology Limited
502#, Block A, Technology Building II, No. 1057, Nanhai Blvd.
Nanshan District, Shenzhen 518067, China
Tel: +86-755-2602 7838 Fax: +86-755-3397 5112

MeSign

Certificates Policy & Practice Statement

Version: 2.0

Status: Final Approved

Release Date：2020-08-18

Effective Date：2020-08-18

MeSign Technology Limited
502#, Block A, Technology Building II, No. 1057, Nanhai Blvd.
Nanshan District, Shenzhen 518067, China
Tel: +86-755-2602 7838 Fax: +86-755-3397 5112

TABLE OF CONTENTS

1. INTRODUCTION 9

1.1. OVERVIEW 9
1.2. DOCUMENT NAME AND IDENTIFICATION 10
1.2.1 Revisions 10
1.3. PKI PARTICIPANTS 10
1.3.1. Certification Authorities 10
1.3.2. Registration Authorities 11
1.3.3. Subscribers 12
1.3.4. Relying Parties 12
1.3.5. Other Participants 12
1.4 CERTIFICATE USAGE 12
1.4.1. Appropriate Certificate Uses 12
1.4.2. Prohibited Certificate Uses 14
1.5 POLICY ADMINISTRATION 14
1.5.1. Organization Administering the Document 14
1.5.2 Contact Person 14
1.5.3 Person Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval Procedures 15
1.6 DEFINITIONS AND ACRONYMS 15
1.6.1. Definitions 15
1.6.2. Acronyms 24
1.6.3 References 25
1.6.4 Conventions 26

2.PUBLICATION AND REPOSITORY RESPONSIBILITIES 26

2.1 REPOSITORIES 26
2.2 PUBLICATION OF CERTIFICATION INFORMATION 27
2.3 TIME OR FREQUENCY OF PUBLICATION 27
2.4 ACCESS CONTROLS ON REPOSITORIES 27

3. IDENTIFICATION AND AUTHENTICATION 28

3.1 NAMING 28
3.1.1. Type of Names 28
3.1.2. Need for Names to be Meaningful 28
3.1.3. Anonymity or Pseudonymity of Subscribers 28
3.1.4. Rules for Interpreting Various Name Forms 28
3.1.5. Uniqueness of Names 29
3.1.6. Recognition, Authentication, and Role of Trademarks 29
3.2 INITIAL IDENTITY VALIDATION 29
3.2.1. Method to Prove Possession of Private Key 29
3.2.2. Authentication of Organization Identity and Domain Identity 29

3.2.3. Authentication of Individual Identity 34
3.2.4. Non-Verified Subscriber Information 35
3.2.5. Validation of Authority 35
3.2.6. Criteria for Interoperation or Certification 36
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 36
3.3.1. Identification and Authentication for Routine Re-Key 36
3.3.2. Identification and Authentication for Re-Key After Revocation 36
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 36

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 36

4.1 CERTIFICATE APPLICATION 36
4.1.1. Who Can Submit a Certificate Application 36
4.1.2. Enrollment Process and Responsibilities 37
4.2 CERTIFICATE APPLICATION PROCESSING 37
4.2.1. Performing Identification and Authentication Functions 37
4.2.2. Approval or Rejection of Certificate Applications 38
4.2.3. Time to Process Certificate Applications 38
4.3 CERTIFICATE ISSUANCE 39
4.3.1. CA Actions During Certificate Issuance 39
4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate 39
4.4 CERTIFICATE ACCEPTANCE 39
4.4.1. Conduct Constituting Certificate Acceptance 39
4.4.2. Publication of the Certificate by the CA 39
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 40
4.5 KEY PAIR AND CERTIFICATE USAGE 40
4.5.1. Subscriber Private Key and Certificate Usage 40
4.5.2. Relying Party Public Key and Certificate Usage 40
4.6 CERTIFICATE RENEWAL 40
4.6.1. Circumstances for Certificate Renewal 41
4.6.2. Who May Request Renewal 41
4.6.3. Processing Certificate Renewal Requests 41
4.6.4. Notification of New Certificate Issuance to Subscriber 41
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 41
4.6.6. Publication of the Renewal Certificate by the CA 41
4.6.7. Notification of Certificate Issuance by the CA to Other Entities 41
4.7 CERTIFICATE RE-KEY 41
4.7.1. Circumstances for Certificate Re-Key 41
4.7.2. Who May Request Certification of a New Public Key 42
4.7.3. Processing Certificate Re-Keying Requests 42
4.7.4. Notification of New Certificate Issuance to Subscriber 42
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 42
4.7.6. Publication of the Re-Keyed Certificate by the CA 42
4.7.7. Notification of Certificate Issuance by the CA to Other Entities 42
4.8 CERTIFICATE MODIFICATION 42

4.8.1. Circumstances for Certificate Modification 42
4.8.2. Who May Request Certificate Modification 42
4.8.3. Processing Certificate Modification Requests 43
4.8.4. Notification of New Certificate Issuance to Subscriber 43
4.8.5. Conduct Constituting Acceptance of Modified Certificate 43
4.8.6. Publication of the Modified Certificate by the CA 43
4.8.7. Notification of Certificate Issuance by the CA to Other Entities 43
4.9 CERTIFICATE REVOCATION AND SUSPENSION 43
4.9.1. Circumstances for Revocation 43
4.9.2. Who Can Request Revocation 45
4.9.3. Procedure for Revocation Request 45
4.9.4. Revocation Request Grace Period 45
4.9.5. Time Within Which CA Must Process the Revocation Request 45
4.9.6. Revocation Checking Requirements for Relying Parties 46
4.9.7. CRL Issuance Frequency 46
4.9.8. Maximum Latency for CRLs 46
4.9.9. On-Line Revocation/Status Checking Availability 46
4.9.10. On-Line Revocation Checking Requirements 46
4.9.11. Other Forms of Revocation Advertisements Available 47
4.9.12. Special Requirements Related to Key Compromise 47
4.9.13. Circumstances for Suspension 47
4.9.14. Who Can Request Suspension 47
4.9.15. Procedure for Suspension Request 47
4.9.16. Limits on Suspension Period 47
4.10 CERTIFICATE STATUS SERVICES 48
4.10.1. Operational Characteristics 48
4.10.2. Service Availability 48
4.10.3. Operational Features 48
4.11 END OF SUBSCRIPTION 48
4.12 KEY ESCROW AND RECOVERY 48
4.12.1. Key Escrow and Recovery Policy and Practices 48
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 49

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 50

5.1 PHYSICAL CONTROLS 50
5.1.1. Site Location and Construction 50
5.1.2. Physical Access 50
5.1.3. Power and Air Conditioning 50
5.1.4. Water Exposures 50
5.1.5. Fire Prevention and Protection 50
5.1.6. Media Storage 51
5.1.7. Waste Disposal 51
5.1.8. Off-Site Backup 51
5.2 PROCEDURAL CONTROLS 51

5.2.1. Trusted Roles 51
5.2.2. Number of Persons Required per Task 51
5.2.3. Identification and Authentication for Each Role 52
5.2.4. Roles Requiring Separation of Duties 52
5.3 PERSONNEL CONTROLS 52
5.3.1 Qualifications, Experience, and Clearance Requirements 52
5.3.2 Background Check Procedures 53
5.3.3 Training Requirements 53
5.3.4 Retraining Frequency and Requirements 54
5.3.5. Job Rotation Frequency and Sequence 54
5.3.6. Sanctions for Unauthorized Actions 54
5.3.7. Independent Contractor Requirements 54
5.3.8. Documentation Supplied to Personnel 54
5.4 AUDIT LOGGING PROCEDURES 55
5.4.1. Types of Events Recorded 55
5.4.2. Frequency for Processing and Archiving Audit Logs 56
5.4.3. Retention Period for Audit Log 56
5.4.4. Protection of Audit Log 56
5.4.5. Audit Log Backup Procedures 56
5.4.6. Audit Collection System (Internal vs. External) 56
5.4.7. Notification to Event-Causing Subject 56
5.4.8. Vulnerability Assessments 57
5.5 RECORDS ARCHIVAL 57
5.5.1. Types of Records Archived 57
5.5.2. Retention Period for Archive 57
5.5.3. Protection of Archive 58
5.5.4. Archive Backup Procedures 58
5.5.5. Requirements for Time-Stamping of Records 58
5.5.6. Archive Collection System (Internal or External) 58
5.5.7. Procedures to Obtain and Verify Archive Information 58
5.6 KEY CHANGEOVER 58
5.7 COMPROMISE AND DISASTER RECOVERY 59
5.7.1. Incident and Compromise Handling Procedures 59
5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted 60
5.7.3. Recovery procedures after Key Compromise 60
5.7.4. Business Continuity Capabilities After a Disaster 60
5.8 CA OR RA TERMINATION 60

6. TECHNICAL SECURITY CONTROLS 61

6.1 KEY PAIR GENERATION AND INSTALLATION 61
6.1.1. Key Pair Generation 61
6.1.2. Private Key Delivery to Subscriber 62
6.1.3. Public Key Delivery to Certificate Issuer 62
6.1.4. CA Public Key Delivery to Relying Parties 62

6.1.5. Key Sizes 62
6.1.6. Public Key Parameters Generation and Quality Checking 62
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field) 62
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 63
6.2.1. Cryptographic Module Standards and Controls 63
6.2.2. Private Key (n out of m) Multi-Person Control 63
6.2.3. Private Key Escrow 63
6.2.4. Private Key Backup 63
6.2.5. Private Key Archival 64
6.2.6. Private Key Transfer into or From a Cryptographic Module 64
6.2.7. Private Key Storage on Cryptographic Module 64
6.2.8. Activating Private Key 64
6.2.9. Deactivating Private Key 64
6.2.10. Destroying Private Key 64
6.2.11. Cryptographic Module Capabilities 65
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 65
6.3.1. Public Key Archival 65
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 65
6.4 ACTIVATION DATA 65
6.4.1. Activation Data Generation and Installation 65
6.4.2. Activation Data Protection 66
6.4.3. Other Aspects of Activation Data 66
6.5 COMPUTER SECURITY CONTROLS 66
6.5.1. Specific Computer Security Technical Requirements 66
6.5.2. Computer Security Rating 66
6.6 LIFE CYCLE TECHNICAL CONTROLS 66
6.6.1. System Development Controls 66
6.6.2. Security Management Controls 67
6.6.3. Life Cycle Security Controls 67
6.7 NETWORK SECURITY CONTROLS 67
6.8 TIME STAMPING 67

7. CERTIFICATE, CRL, AND OCSP PROFILES 68

7.1 CERTIFICATE PROFILE 68
7.1.1 Version Number(s) 68
7.1.2 Certificate Extensions 68
7.1.3 Algorithm Object Identifiers 72
7.1.4 Name Forms 72
7.1.5 Name Constraints 72
7.1.6 Certificate Policy Object Identifier 73
7.1.7 Usage of Policy Constraints Extension 73
7.1.8 Policy Qualifiers Syntax and Semantics 74
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 74
7.2 CRL PROFILE 74

7.2.1 Version Number(s) 74
7.2.2 CRL and CRL Entry Extensions 74
7.3 OCSP PROFILE 74
7.3.1 Version Number(s) 74
7.3.2 OCSP Extensions 74

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 75

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT 75
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 75
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 75
8.4 TOPICS COVERED BY ASSESSMENT 76
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 76
8.6 COMMUNICATIONS OF RESULTS 76
8.7 SELF-AUDITS 76

9. OTHER BUSINESS AND LEGAL MATTERS 77

9.1 FEES 77
9.1.1. Certificate Issuance or Renewal Fees 77
9.1.2. Certificate Access Fees 77
9.1.3. Revocation or Status Information Access Fees 77
9.1.4. Fees for Other Services 77
9.1.5. Refund Policy 77
9.2 FINANCIAL RESPONSIBILITY 77
9.2.1. Insurance Coverage 77
9.2.2. Other Assets 78
9.2.3. Insurance or Warranty Coverage for End-Entities 78
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 78
9.3.1. Scope of Confidential Information 78
9.3.2. Information Not Within the Scope of Confidential Information 79
9.3.3. Responsibility to Protect Confidential Information 79
9.4 PRIVACY OF PERSONAL INFORMATION 79
9.4.1. Privacy Plan 79
9.4.2. Information Treated as Private 79
9.4.3. Information Not Deemed Private 79
9.4.4. Responsibility to Protect Private Information 79
9.4.5. Notice and Consent to Use Private Information 80
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 80
9.4.7. Other Information Disclosure Circumstances 80
9.5 INTELLECTUAL PROPERTY RIGHTS 80
9.6 REPRESENTATIONS AND WARRANTIES 80
9.6.1. CA Representations and Warranties 80
9.6.2. RA Representations and Warranties 81
9.6.3. Subscriber Representations and Warranties 82
9.6.4. Relying Party Representations and Warranties 82

9.6.5. Representations and Warranties of Other Participants 83
9.7 DISCLAIMERS OF WARRANTIES 83
9.8 LIMITATIONS OF LIABILITY 84
9.9 INDEMNITIES 84
9.9.1 Indemnification by MeSign 84
9.9.2 Indemnification by Subscribers 84
9.9.3. Indemnification by Relying Parties 85
9.10 TERM AND TERMINATION 85
9.10.1. Term 85
9.10.2. Termination 85
9.10.3. Effect of Termination and Survival 85
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 85
9.12 AMENDMENTS 86
9.12.1. Procedure for Amendment 86
9.12.2. Notification Mechanism and Period 86
9.12.3. Circumstances Under Which OID Must be Changed 86
9.13 DISPUTE RESOLUTION PROVISIONS 86
9.14 GOVERNING LAW 87
9.15 COMPLIANCE WITH APPLICABLE LAW 87
9.16 MISCELLANEOUS PROVISIONS 87
9.16.1. Entire Agreement 87
9.16.2. Assignment 87
9.16.3. Severability 87
9.16.4. Enforcement (attorney's fees and waiver of rights) 87
9.16.5. Force Majeure 88
9.17 OTHER PROVISIONS 88

1. Introduction

1.1. Overview

This document is the MeSign Certification Practice Statement (CPS) and outlines the legal, commercial and technical principles and practices that MeSign employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based Public Key Infrastructure (PKIX) in accordance with this Certificate Policies determined by MeSign. It also defines the underlying certification processes for Subscribers and describes MeSign' repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the MeSign PKI.

The current and successive versions of this document intend to meet or exceed the requirements of the WebTrust Requirements for the Issuance and Management of Publicly Trusted Certificates.

For client certificates, MeSign conforms to the Adobe AATL Certificate Policy, if there is any inconsistency between this document and the Adobe AATL Certificate Policy, the Policy Requirements take precedence over this document.

In case multiple or alternative methods or options are possible by the baseline requirements or guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to those requirements and guidelines, MeSign reserves the right to choose any of the methods or options applicable at any times and may choose to change its procedures at all times and decide to do so on a case to case basis.

In pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this document is divided into nine parts that cover the security controls and practices and procedures for certificate and time stamping services within the MeSign PKI. To preserve the outline specified by RFC 3647, sections that do not apply have the statement "Not applicable" or "No stipulation."

MeSign may publish additional certificate policies or certification practice statements as necessary to describe other product and service offerings. These supplemental policies and statements are available to applicable users or relying parties through the online repositories.

1.2. Document Name and Identification

This document is the MeSign CA Certification Practice Statement. MeSign OID is described in section 7.1.6 of this document.

1.2.1 Revisions

Ver.	Description	Adopted	Effective
1.0	Version 1.0 of the Certificate Practice Statement Adopted	2018.01.22	2018.01.22
1.1	Correct some mistakes	2018.12.13	2018.12.13
2.0	Setup an independent CPS	2020.08.18	2020.08.18

1.3. PKI Participants

1.3.1. Certification Authorities

MeSign Technology Limited is incorporated and registered in China. General information about MeSign products and services are available at www.mesign.com.

MeSign is a Certification Authority (CA) that issues high quality and highly trusted digital certificates to entities including private and public companies and individuals in accordance with this CPS. In its role as a CA, MeSign performs functions associated with Public Key operations that include receiving requests, issuing, revoking and renewing a digital certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the MeSign PKI. In delivering its PKI services MeSign complies in all material respects with high-level international standards.

MeSign' offline self-signed Root CAs issue CA Certificates to subordinate CAs in accordance with this CPS. MeSign owns and operates the following Root CAs that can be download at https://www.mesign.com/root/.

Root CA 1:

Common Name: MeSince Identity CA
Organization: MeSince Technology Limited
Serial Number: 3FEF239ECCC031FDDF664E3A1726B8C4
Fingerprint: BE5E323A6E608652ED0113CBB8F92FF9768ABDCC

Root CA 2:

Common Name: MeSign Identity CA
Organization: MeSign Technology Limited
Serial Number: 2DC7D9846C26D202EDBBA2E6F3207DC9
Fingerprint: 23AAC780C2C6A50BBD0B42B07FAD20A6ED55E143

MeSign have issued several intermediate root CAs from above 2 Root CAs, and the detailed information about those intermediate root CA (Issuing CA) is listed at:
https://www.mesign.com/root/.

1.3.2. Registration Authorities

Not applicable.

1.3.3. Subscribers

Subscribers of MeSign services are individuals or organizations that use PKI in relation with MeSign supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the Private Key corresponding to the Public Key listed in the certificate. Prior to verification of identity and issuance of a certificate, a subscriber is an Applicant for the services of MeSign. Each Subscriber must agree the Subscriber Agreement with MeSign in related online page.

1.3.4. Relying Parties

Relying parties use PKI services in relation with MeSign certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a Public Key listed in a subscriber certificate.

Relying parties must refer to the Certificate Revocation List (CRL) prior to replying on information featured in a certificate to ensure that it has not been revoked. CRL location is detailed within each certificate.

1.3.5. Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1. Appropriate Certificate Uses

By accepting a certificate from MeSign, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this document and relevant policies. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for

signing). Subscribers shall protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation. That means that legislation will decide on a case by case base whether or not they are legally binding. Because of these legal implications, subscribers must protect their Private Keys.

Renewing a certificate follows the same procedures as with a new certificate. Re-keying or reusing the same Private Key for any new or renewed certificate shall be avoided by the subscriber.

1.4.1.1. Certificate Types

Client Certificates are typically used for authentication purpose, signing and encryption of electronic mail and digital documents. They are also referred to as S/MIME certificate and may be applicable for one or more purposes mentioned above depending on the key usage limit specified in the certificate.

Time Stamping Certificates are used to ensure that the signing event took place at a specific point in time.

Intermediate CA Certificates are used exclusively for the issuing and signing of end user certificates and Certificate Revocation Lists. Each CA certificate is responsible for the signing of a different validation level and different purpose.

CA Root Certificate is used to exclusively sign and issue the intermediate CA certificates and corresponding Certificate Revocation List.

1.4.1.2. Certificate Validation Level

V1 Certificate provides modest assurances that the email originated from a sender with the specified email address or that the domain address belongs to the respective server address. These certificates provide no proof of the identity of the subscriber or of the organization. V1 certificates are limited to client. In some document, this level certificate is named as Class 1 certificate.

V2 Certificate provides medium assurances about the subscriber's identity and subscribers must prove their identity by various means, this level certificate is for individual only. In some document, this level certificate is named as Class 2 certificate.

V3 Certificate, for client certificate, it provides a high level of assurance about the subscriber's identity and are issued only to organizations to which the MeSign has validated

the organization identity by phone call and/or by third party authority trusted database.

V4 Certificate, for client certificate, it provides an extended validation of high level assurance about the subscriber's identity as one of the employee of an organization.

1.4.2. Prohibited Certificate Uses

Certificates issued under the provisions of this CPS may not be used for: (i) any application requiring failsafe performance such as: (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of encryption or digital certificates for such transactions or where otherwise prohibited by law.

1.5 Policy Administration

1.5.1. Organization Administering the Document

This CPS and the documents referenced herein are maintained by the MeSign Certificate Policy Authority (MCPA), which can be contacted at:

MeSign Policy Authority
502#, Block A, Shekou Technology Building II, No. 1057, Nanhai Blvd
Nanshan District, Shenzhen 518067, China
Tel: +86-755-86008688
Fax: +86-755-33975112
Website: www.mesign.com
Email: cps@mesign.com

1.5.2 Contact Person

Attn: Legal Counsel
MeSign Policy Authority
502#, Block A, Shekou Technology Building II, No. 1057, Nanhai Blvd
Nanshan District, Shenzhen 518067, China
website: www.mesign.com
Email: cps@mesign.com

1.5.2.1 Revocation Reporting Contact Person

Attn: Risk Control Team
502#, Block A, Shekou Technology Building II, No. 1057, Nanhai Blvd Nanshan District, Shenzhen 518067, China
website: www.mesign.com

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. MeSign will authenticate and log each revocation request according to Section 4.9 of this CPS. MeSign will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, MeSign will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3.

1.5.3 Person Determining CPS Suitability for the Policy

The MCPA is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

1.5.4 CPS Approval Procedures

The MCPA approves the CPS and any amendments. Upon the MCPA accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the MeSign repository (available at http://www.mesign.com/policy/). And controls are in place to reasonably ensure that the MeSign CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

1.6 Definitions and Acronyms

All other definitions and acronyms are according to the related WebTrust Guidelines.

1.6.1. Definitions

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (http), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Business Entity: Any entity that is not a Private Organization, Government Entity, or non-commercial entity as defined in the EV Guidelines. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CAA: From RFC 6844 (http://tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS Domain Name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

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

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate System Component: A individual element of a larger Certificate System used to process, approve issuance of, or store certificates or certificate status information. This includes the database, database server, storage devices, certificate hosting services, registration authority systems, and any other element used in certificate management.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Transparency (CT): Publicly operated record of certificate issuance.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

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

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

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their Affiliates, contractors, delegates, successors, or assigns).

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated Legal Entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Hardware Security Module (HSM): An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

High Security Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the CA's or Delegated Third Party Private Key or cryptographic hardware.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical

technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair .

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

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

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

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

Parent Company: A company that Controls a Subsidiary Company.

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.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.3.

Qualified Government Information Source: A database maintained by a Government Entity.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

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

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at https://www.mesign.com/policy/.

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

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

- The Request Token SHALL incorporate the key used in the certificate request.
- A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness.
- A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
- A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.
- A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements found in this document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.

Security Support Systems: A system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus.

Signed Certificate Timestamp (SCT): A timestamp and promise from a Certificate Transparency operator to add the submitted certificate to the log within a specified time period.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or Subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subject AltName extension or the subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Test Certificate: A Certificate with a maximum Validity Period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a Root Certificate Subject to these Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce

the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

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

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

Zone: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

1.6.2. Acronyms

AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EKU	Extended Key Usage

EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology OCSP Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

1.6.3 References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

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 TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing Public Key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements for Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public Key infrastructure for financial services – Practices and policy framework.

Network and Certificate System Security Requirements, v.1.0, 1/1/2013.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications,
http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, January 2013.

WebTrust for Certification Authorities, SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.4 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements shall be interpreted in accordance with RFC 2119.

2.Publication and Repository Responsibilities

2.1 Repositories

MeSign publishes a repository of legal notices regarding its PKI services, including this CPS, certificates, CRLS, agreements and notices, references within this CPS as well as any other information it considers essential to its services.

The MeSign legal repository may be accessed at https://www.mesign.com/policy/. MeSign' root Certificates and its CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime.

2.2 Publication of Certification Information

MeSign manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by MeSign are X.509v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. The CRL distribution points are included in the certificates.

2.3 Time or Frequency of Publication

CA Certificates are published in a repository as soon as possible after issuance. MeSign updates and publishes a new CRL every 48 hours or whenever a CA Certificate is revoked. The CRL of root and intermediate CA certificates may be valid for one year and shall be updated accordingly.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain published available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate
New or modified versions of the CP/CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

This CPS is updated at least once every year. Even if no other changes are made to the contents of this CPS, MeSign will increment the version number and update the release date, effective date, and the revision records of this CPS.

2.4 Access Controls on Repositories

Read-only access to the repository is unrestricted. Logical and physical controls prevent

unauthorized write access to repositories.

3. Identification and Authentication

3.1 Naming

3.1.1. Type of Names

MeSign Certificates are issued with Subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading. However, some Certificates Common Names may also include RFC2460 (IP version 6) or RFC791 (IP version 4) addresses.

3.1.2. Need for Names to be Meaningful

MeSign uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the Subject of the Certificate and the entity that is the issuer of the Certificate.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, MeSign does not issue anonymous or pseudonymous Certificates; however, for IDNs, MeSign may include the Punycode version of the IDN as a Subject name. MeSign may also issue other pseudonymous end-entity certificates if they are allowed by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of Names

Name uniqueness is ensured through the use of either the Common Name attribute of the Subject Field for server certificates, the emailAddress attribute of the Subject Field for S/MIME certificates and the Common Name and Organization attribute of the Subject Field for code signing certificates.

3.1.6. Recognition, Authentication, and Role of Trademarks

MeSign performs sanity and fraud prevention checks in order to limit accidental issuing of certificates whose domain or organization names might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks.

Subscribers may not request Certificates with any content that infringes the intellectual property rights of a third party. MeSign does not require that an Applicant's right to use a trademark be verified. MeSign reserves the right to revoke any Certificate that is involved in a dispute.

3.2 Initial Identity Validation

MeSign may perform identification of the Applicant or for services including CA chaining services using any legal means of communication or investigation necessary to identify the Legal Entity or individual. MeSign may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered either as a Certificate Signing Request (CSR) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

The V1 encryption certificate Private Key is generated in MeSign Key Management System (FIPS140-2 Level 3 HSM) and stored in KM system securely, and the signing certificate Private Key is generated in user's device and post CSR to CA system to get the certificate.

3.2.2. Authentication of Organization Identity and Domain Identity

3.2.2.1. Identity

MeSign manually performs the organization's authentication process, in addition to verifying the correctness of the organization's information and verifying that the certificate Applicant is a duly authorized certificate Applicant.

MeSign verifies the identity and address of the Applicant using: Effective documents issued by government agencies, including but not limited to business licenses, organization code certificate, etc., or through the issuance of valid documents to verify the authority of the third-party database.

MeSign may verify the correctness of the organization details through payment transactions to its bank account by the subscriber. The transaction details must explicitly include the correct organization details of the subscriber. Additionally, MeSign obtains through third party records a phone number that is owned by the organization and by performing a

verification call. During the verification call MeSign establishes the authority of the subscriber.

MeSign will also check the authorization documents authorized by the agency to the certificate Applicant for the certificate and the valid identity document of the authorized person.

Depending on the type of certificate, there are some differences in the steps for MeSign to perform authentication. In general, the higher the security level of the certificate, the more stringent the authentication is.

1) Authentication of Client Certificates

   For Client certificates, according to different validation level, we will verify the Applicant's right to use or control the email address and verify the Applicant identity, see Section 3.2.2.8 for verification.

2) Organization Validation

   The authorized applicant (Requester) is required to submit one or more of the following proof documents. These documents include:

   (1) Registration document issued by government, e.g. business license, Certificate of Organization Code etc.;(Optional)

   (2) Operational existence evidence, e.g. bank account certification, bank statement, utility bills, leasing contract etc.; (Optional)

   (3) Subscriber Agreement and Authorization Letter sealed and/or signed by the Application Approver;

   Our Validation Officers will check in government agency website in the jurisdiction of the applicant, to verify the authenticity of the organization information from the submitted legitimated proof documents.

   Apart from that, the Validation Officers will verify the consistency of the organization information in different documents to confirm the operational existence of the organization. Then, they will make vetting phone call using the phone number provided in the Subscriber Agreement and Authorization Letter, or the phone number from telephone company directory, Baidu Map, Google Map and other reliable resource, to confirm with the Application Approver, the authorization to the applicant, and to ask him to provide the Authorization Code. In the case that phone vetting is unavailable, our Validation Officer will ask the Application Approver to send the Authorization Code to vo@mesign.com for validation.

   Validation Officer must validate the email account domain is belong to the organization

3.2.2.2. DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, MeSign verifies that

the Applicants have right to use the DBA/tradename using at least one of the followings:

1) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2) A Reliable Data Source;
3) Communication with a government agency responsible for the management of such DBAs or tradenames;
4) An Attestation Letter accompanied by documentary support; or
5) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that MeSign determines to be reliable.

3.2.2.3. Verification of Country

If the Subject: countryName field is present, MeSign verify the country associated with the Subject using one of the followings:

1) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;
2) information provided by the Domain Name Registrar;

3.2.2.4 Validation of Domain Authorization or Control

MeSign confirm that prior to issuance, has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

3.2.2.4.1 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The email address must use the WHOIS records provided by the Domain Registrar, the Applicant can use the email address to receive a Random Value if the WHOIS date contains an administrative email address.

Each email MAY confirm control of multiple Authorization Domain Names.

MeSign MAY send the email identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email.

The Random Value SHALL be unique in each email.

If the communication's entire contents and recipient(s) remain unchanged, MeSign MAY resend the email in its entirety, including re-use of the Random Value.

The Random Value SHALL remain valid for use in a confirming response for no more than 7 days from its creation.

Note: Once the FQDN has been validated using this method, MeSign MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.2 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value SHALL be unique in each email.

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.

The Random Value SHALL remain valid for use in a confirming response for no more than 7 days from its creation.

Note: Once the FQDN has been validated using this method, MeSign MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Domain Authorization Document

Confirming the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The validation officer from MeSign verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

3.2.2.4.4 Agreed-Upon Change to Website

N/A

3.2.2.4.5 DNS Change

N/A

3.2.2.5. Authentication for an IP Address

N/A

3.2.2.6 Wildcard Domain Validation

N/A

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, MeSign will evaluate the source for its reliability, accuracy, and resistance to alteration or falsification, and consider the following during evaluation:

(1) The age of the information provided,

(2) The frequency of updates to the information source,

(3) The data provider and purpose of the data collection,

(4) The public accessibility of the data availability, and

(5) The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

N/A

3.2.3. Authentication of Individual Identity

MeSign manually performs the personal identities authentication process, verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

MeSign verifies the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver license, military ID, national ID, or equivalent document type).

MeSign verifies the Applicant's address using a form of identification that MeSign determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. MeSign MAY rely on the same government-issued ID that was used to verify the Applicant's name.

MeSign verifies the certificate request with the Applicant by sending emails or making phone calls etc.

Depending on the type of certificate, there are some differences in the steps for MeSign to perform authentication. In general, the higher the security level of the certificate, the more stringent the authentication is.

1) Authentication of Client Certificates

For Client certificates, in addition to verifying the Applicant's name, also need to verify the Applicant's right to use or control the email address.

Email accounts are validated by sending an electronic mail message with a verification code to the requested email account. The subscriber must return and submit the verification code as prove of ownership of the email account within a limited period sufficient enough to receive an electronic mail message.

2) Individual Validation

The subscriber must use MeSign APP to take a photo in which he/she holds his/her ID card (both sides) or passport, and upload it via MeSign APP. In addition, he needs to upload a second proof document like passport, social security card, driver license, or other valid document issued by government.

For Chinese subscriber, no need to provide any proof document, just need to use MeSign APP to pass the face recognition authentication, and If the subscriber fails to pass this authentication, he/she must follow the verification requirements of the first section.

The Validation Officers will verify the applicant is truly the identity he/she claims according to the picture of "holding ID card". Meanwhile, our Validation Officers will compare the personal information on other identity document with the information in the picture of "holding ID card" to confirm the authenticity of the identity information.

The validation may be valid for 7 days for the generation of digital certificates.

3.2.4. Non-Verified Subscriber Information

MeSign does not verify the following subscriber information:

- Organizational Unit (OU);
- Organization-specific information not used for identification purposes;
- Other information designated as non-verified in the certificate；
- The first name in other language except its ID language in V2/V3/V4 Signing Certificate.

3.2.5. Validation of Authority

MeSign confirms and verifies that the Applicant Representative is duly authorized to represent the organization and obtain the certificates on their behalf by obtaining an authorization statement and by contacting the authorizer. The obtained and confirmed organization documents should state the authorizer and position, but MeSign may rely on other means and sources to obtain the necessary authority if necessary. MeSign may assume proper authorization in case the validated subscriber is either the appointed CEO, Director, President or owner and sole proprietor.

MeSign allows an Applicant to specify individuals to request certificates. If an Applicant specifies, in writing, the individuals who may request a certificate, then MeSign does not accept any certificate requests that are outside this specification. MeSign provides an Applicant with a list of its authorized certificate requests upon the Applicant's verified written request.

3.2.6. Criteria for Interoperation or Certification

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Subscribers should not reuse Private Keys for successive certificates after expiration thereof and it's highly recommended to create a new key for every certificate.

3.3.2. Identification and Authentication for Re-Key After Revocation

Private Keys of certificates which were revoked should not be reused.

3.4 Identification and Authentication for Revocation Request

See Sections 4.9.1 through 4.9.3 for information about Certificate revocation procedures.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1. Who Can Submit a Certificate Application

Any individual who is the Subject of the certificate or any authorized representative of an Organization or entity.
MeSign SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. MeSign SHALL use this information to identify subsequent suspicious certificate requests.

4.1.1.1. Subscriber Agreement Requirements

By accepting a certificate from MeSign, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this CP and the relevant CP statements. The certificate Applicants can acknowledge the acceptance of CP and CPS electronically on MeSign website. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the certificate.

4.1.1.2. Certificate Request Requirements for DV/IV/OV/EV SSL Certificates

N/A

4.1.2. Enrollment Process and Responsibilities

MeSign maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow MeSign to successfully perform the required verification. MeSign shall protect communications and securely store information presented by the Applicant during the application process in compliance with the MeSign Privacy Policy.

In no particular order, the enrollment process includes:

1) Generating a suitable Key Pair using a suitably secure platform;
2) Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
3) Submitting a request for a Certificate type and appropriate application information;
4) Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
5) Paying any applicable fees.

4.2 Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

MeSign maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CPS. Initial vetting may be performed by MeSign' validation team as set forth in Section 3.2. All communications sent through as email are securely stored along with all information presented directly by the Applicant via the MeSign web interface or API. Future applications for Certificates are authenticated using single (username and password) or multi-factor (Certificate in combination with

username/password) authentication techniques.

4.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application, MeSign approves an application for a digital certificate.

If the validation of a certificate application fails, MeSign rejects the certificate application. MeSign reserves the right to reject applications to issue a certificate to Applicants if, on its own assessment and may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. Applicants whose applications have been rejected may subsequently re-apply.

MeSign may reject requests based on potential brand damage to MeSign in accepting the request. MeSign may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement. MeSign is under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

MeSign makes reasonable efforts to confirm certificate application information and issue the Certificates within a reasonable time frame. This greatly dependents on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, MeSign aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application.

The following is the approximate processing time:

V1 Client Certificates	30 minutes
V2 Client Certificates	one business day
V3 Client Certificates	one business day
V4 Client Certificates	one business day

4.3 Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

MeSign offers different certificate types to make use of S/MIME technology for secure

online transactions, secure electronic file and secure email respectively. Prior to the issuance of a certificate, MeSign will validate an application in accordance with this CPS which may involve the request by MeSign to the Applicant for relevant official documentation supporting the application.

MeSign does not issue end entity certificates directly from its Root Certificates. MeSign logs its issued SSL Certificates in two or more Certificate Transparency databases. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

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

MeSign shall notify the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrollment process or by any other equivalent method. The email may contain the Certificate itself or a link to download depending upon the workflow of the Certificate requested.

4.4 Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

MeSign shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies MeSign within seven (7) days from receipt, the Certificate is deemed accepted.

4.4.2. Publication of the Certificate by the CA

MeSign publishes all CA Certificates in its repository (https://www.mesign.com/root). MeSign publishes end-entity Certificates by delivering them to the Subscriber.

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

No other publication or notification to others occurs.

4.5 Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation. That means that legislation will decide on a case by case base whether or not they are legally binding. Because of these legal implications, subscribers must protect their Private Keys.

For all subscriber encryption certificates issued from the Root 4 listed in 1.3.1, the Private Key is generated in CA Key Management system with a FIPS 140-2 Level 3 certified HSM, and the Private Key is divided into two parts, encrypted and stored in two different key management servers. After the Private Key and Public Key certificate are installed in APP, it is securely stored in the APP.

4.5.2. Relying Party Public Key and Certificate Usage

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, relying parties shall independently assess:

1) That the certificate is being used in accordance with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
2) The status of the end entity certificate and all the CA certificates in the chain that issued the certificate. If any of the certificates in the certificate chain have been revoked, the relying party shall not rely on the end user certificate or other revoked certificates in the certificate chain.

4.6 Certificate Renewal

Renewing a certificate follows the same procedures as with a new certificate.

4.6.1. Circumstances for Certificate Renewal

Not applicable.

4.6.2. Who May Request Renewal

Not applicable.

4.6.3. Processing Certificate Renewal Requests

Not applicable.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6. Publication of the Renewal Certificate by the CA

Not applicable.

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

Not applicable.

4.7 Certificate Re-Key

MeSign treats certificate re-key requests as requests for the issuance of a new Certificate. Re-keying or reusing the same Private Key for any new or renewed certificate shall be avoided by the subscriber.

4.7.1. Circumstances for Certificate Re-Key

Not applicable.

4.7.2. Who May Request Certification of a New Public Key

Not applicable.

4.7.3. Processing Certificate Re-Keying Requests

Not applicable.

4.7.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

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

Not applicable.

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

Not applicable.

4.8 Certificate Modification

MeSign does not modify previously issued certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

4.8.1. Circumstances for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not applicable.

4.8.3. Processing Certificate Modification Requests

Not applicable.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6. Publication of the Modified Certificate by the CA

Not applicable.

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

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated Validity Period. A certificate will be revoked when the information it contains is suspected to be incorrect or compromised.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

MeSign will revoke a Subscriber Certificate within 24 hours if one or more of the following occurs:

1) The Subscriber requests in writing that MeSign revoke the Certificate;
2) The Subscriber notifies MeSign that the original certificate request was not authorized and does not retroactively grant authorization;
3) MeSign obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4) MeSign obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

MeSign may revoke a certificate within 24 hours and will revoke a Certificate within 5 days if one or more of the following occurs:

1) The Certificate no longer complies with the requirements of related requirements;
2) MeSign obtains evidence that the Certificate was misused;
3) The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4) MeSign confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
5) MeSign confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6) MeSign confirms a material change in the information contained in the Certificate;
7) MeSign confirms that the Certificate was not issued in accordance with the CA/B

forum requirements or this CPS;

8) MeSign determines or confirms that any of the information appearing in the Certificate is inaccurate;
9) MeSign' right to issue Certificates under the CA/B forum requirements expires or is revoked or terminated, unless MeSign has made arrangements to continue maintaining the CRL/OCSP Repository;
10) Revocation is required by this CPS; or
11) MeSign confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

MeSign will revoke a Subordinate CA Certificate within 7 days if one or more of the following occurs:

1) The Subordinate CA requests revocation in writing;
2) The Subordinate CA notifies MeSign that the original certificate request was not authorized and does not retroactively grant authorization;
3) MeSign obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements;
4) MeSign obtains evidence that the Certificate was misused;
5) MeSign is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6) MeSign determines that any of the information appearing in the Certificate is inaccurate or misleading;
7) MeSign or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8) MeSign' or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless MeSign has made arrangements to continue maintaining the CRL/OCSP Repository; or
9) Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
10) The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

4.9.2. Who Can Request Revocation

Certificate revocation can be requested by the subscriber of the certificate or by any other entity presenting proof of knowledge of circumstances for revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may

submit Certificate Problem Reports informing MeSign of reasonable cause to revoke the certificate. MeSign may also at its own discretion revoke Certificates.

4.9.3. Procedure for Revocation Request

Subscribers may request revocation of a certificate by using the online utility provided at the MeSign website. MeSign makes every reasonable effort to verify the claims, reason and identity of the requester.

The subscriber will be notified of the revocation via electronic mail message. Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded and an updated CRL shall be issued. Notification of revocation of a certificate to others than the subscriber and Subject of the certificate, beyond the published CRL, are generally not performed.

MeSign maintains a continuous 24X7 ability to internally respond to any high priority revocation requests. If appropriate, MeSign forwards complaints to law enforcement.

4.9.4. Revocation Request Grace Period

MeSign may grant and extend revocation grace periods on a case-by-case basis.

4.9.5. Time Within Which CA Must Process the Revocation Request

MeSign maintains 24 x 7 ability to respond internally to a high-priority Certificate Problem Report and, where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the Subject of such a complaint. MeSign will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

Within 24 hours after receiving a Certificate problem report, MeSign investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, MeSign works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which MeSign will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by MeSign will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of

harm);

2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

4.9.6. Revocation Checking Requirements for Relying Parties

Relying parties must verify the certificate against the revocation list (CRL) and/or OCSP Responder, check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

4.9.7. CRL Issuance Frequency

The corresponding Certificate Revocation Lists (CRL) of subscriber certificates are updated at least every 48 hours or every time a certificate is revoked, whichever comes first. The CRL is valid for 5 days. The CRL is published via Internet download. Each intermediate CA issues its own corresponding CRL for the certificates issued. The CRL distribution points are included in the certificates.

The CRL of intermediate CA certificates is updated at least once every twelve (12) months and within 24 hours after revoking an intermediate CA certificate, and the value of the nextUpdate field is not more than 12 months beyond the value of the thisUpdate field.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain published available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate.

4.9.8. Maximum Latency for CRLs

Certificate Revocation Lists is published at the on-line repository within a commercially reasonable time after generation. This is generally done automatically and within three (3) hours after generation of a new CRL.

4.9.9. On-Line Revocation/Status Checking Availability

An OCSP Responder service is provided and the respective URL location of the service is

included in the certificates. The OCSP Responder provides results about the status of a certificate instantly. Error responses by the OCSP Responder may be unsigned and include regular HTTP status errors.

4.9.10. On-Line Revocation Checking Requirements

Relying parties must verify the certificate against the revocation list (CRL) and/or OCSP Responder, check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

For the status of Subscriber Certificates:
MeSign update the OCSP information at least every day. OCSP responses from this service have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:
MeSign update the OCSP information at least every twelve months, and within 24 hours after revoking a Subordinate CA Certificate.

MeSign does not respond with a "good" status for status of a certificate that has not been issued.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

MeSign uses commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where MeSign at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, MeSign shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRLs within one hour of creation.

4.9.13. Circumstances for Suspension

Certificates issued to subscriber may be either valid, expired or revoked. MeSign does not perform certificate suspension and subscribers are advised to request a new certificate in case of expiration or revocation of previously valid certificates.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1. Operational Characteristics

MeSign provides a Certificate status service either in the form of a CRL distribution point or an OCSP Responder or both. For Timestamp Certificates, MeSign does not remove revocation entries on CRL or OCSP after the Expiry Date of the revoked Certificate. For other Certificate types, MeSign does not remove revocation entries on CRL or OCSP after the Expiry Date of the revoked Certificate.

4.10.2. Service Availability

MeSign provides 24x7 certificate status services. except user's network reason, and the response time is of ten seconds or less.

4.10.3. Operational Features

No stipulation.

4.11 End of Subscription

A Subscriber may terminate its subscription to certificate services by allowing the term of a Certificate or applicable agreement to expire without renewal. A Subscriber may also voluntarily revoke a Certificate as explained in Section 4.9.

4.12 Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

For all subscriber's encryption certificates issued from the Root 4 listed in 1.3.1, the Private Key is generated in CA Key Management System with a FIPS 140-2 Level 3 certified HSM, and the Private Key is divided into two parts, encrypted and stored in two different key management servers. The encryption certificate Private Key is managed and secure saved by MeSign, and the signature certificate Private Key is kept by subscriber. When a new device used MeSign APP, the encryption Private Key and Public Key certificate will be installed in the new device automatically after finishing the email control validation and entering the correct Private Key protection password if set.

MeSign never escrows CA Private Keys.

MeSign may escrow Subscriber's encryption certificate Private Key to provide key recovery services. MeSign encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key.

MeSign allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys.
MeSign uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. MeSign accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the Private Key;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with MeSign for Private Key escrow;
3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with MeSign for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using MeSign' key escrow services are required to:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request
5. for recovery; and
6. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key related information, or the facts concerning any key recovery request or process.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1. Site Location and Construction

MeSign has two machine rooms in Beijing and Shenzhen, all sites operate under a security policy designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities. Physical barriers are used to segregate secure areas within buildings and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry. External walls of the site are of solid construction.

5.1.2. Physical Access

The hardware is located in a dedicated, resistant server room. Access to the facility by individuals (personnel and others) is strictly controlled and restricted to authorized and trusted personnel only. Maintenance and other services applied to the cryptographic devices and server systems must be authorized by the CEO or CTO of MeSign or equally authorized caretaker of the MeSign PKI. Physical access to the server infrastructure and facilities shall be logged and signed by at least one other witness on the four eyes principal. Otherwise physical access to the systems shall be avoided.

5.1.3. Power and Air Conditioning

The locality is fully air conditioned to prevent overheating and to maintain a suitable humidity level. Primary and secondary power supplies ensure continuous, uninterrupted access to electric power. Electricity power backup (UPS) is supported by an external, independent electricity power source for cases of prolonged power outages.

5.1.4. Water Exposures

All server equipment and devices are elevated above the ground. No water lines exist above equipment.

5.1.5. Fire Prevention and Protection

Fire alarm and intrusion prevention equipment are installed, maintained and available at the premise.

5.1.6. Media Storage

The server room is monitored by a closed-circuit camera and television monitoring system with recording capabilities and records shall be archived in a rolling and increasing mode.

Daily backup of its CA related data that are rotated and stored according to either on-site or off-site according to an established backup rotation schedule.

5.1.7. Waste Disposal

MeSign implemented procedures for the disposal of waste (paper, media, or any other waste) in order to prevent the unauthorized use of, or access to, or disclosure of waste containing confidential information.

5.1.8. Off-Site Backup

The CA Private Keys and activation data are stored on-site in separate safety vaults accessible only by trusted personnel.

The cloned CA Private Keys HSM and the database is backed up in a rolling fashion and secure manner at an off-site facility beyond 2,000 Kilometer of MeSign' main infrastructure.

5.2 Procedural Controls

5.2.1. Trusted Roles

MeSign follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. Personnel acting in trusted roles include CA, TSA, and CMS system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the MeSign PKI's operations. Trusted roles are appointed by senior management. A list of

personnel appointed to trusted roles is maintained and reviewed annually.

5.2.2. Number of Persons Required per Task

Handling of CA Private Keys (throughout the entire CA key lifecycle) requires the involvement of at least two trusted persons. Physical and logical access controls exist for the key activation material in order to maintain multi-party control over the Hardware Security Modules containing CA Private Keys.

The signing of Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer and in attendance of at least one witness.

5.2.3. Identification and Authentication for Each Role

Personnel in trusted roles must authenticate themselves to CA, TSA, and CMS system before they are allowed access to the components of the system necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

The signing of CA Root Certificates, Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer of MeSign and attendance by at least one witness.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

MeSign employs enough personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. MeSign personnel fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. MeSign personnel (both temporary and permanent) have job descriptions defined from the viewpoint of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. MeSign personnel are formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are

employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

The MCPA is responsible and accountable for MeSign' PKI operations and ensures compliance with this CPS. MeSign' personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

Management and operational support personnel involved in timestamp operations possess experience with information security and risk assessment and knowledge of timestamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. The MCPA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2 Background Check Procedures

MeSign verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. MeSign requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., resident identity card and/or passports etc.). Background checks include employment history, education and criminal background. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources administration department makes an adjudication decision, as to whether the individual is suitable for the position to which they will be assigned.

MeSign requires that all individuals assigned to trusted roles to provide proof non-criminal record or non-criminal statement every year.

5.3.3 Training Requirements

MeSign provides skills training to all employees involved in MeSign' PKI and CMS operations. The training relates to the person's job functions and covers:

1) basic Public Key Infrastructure (PKI) knowledge,
2) software versions used by MeSign,
3) authentication and verification policies and procedures,
4) MeSign security principals and mechanisms,
5) disaster recovery and business continuity procedures,
6) common threats to the validation process, including phishing and other social

engineering tactics, and

7) applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

MeSign maintains records of who received training and what level of training was completed. Validation Specialist must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Validation Specialist are required to pass an internal examination on the MeSign Validation Operational Guide prior to validating and approving the issuance of Certificates.
Where competence is demonstrated in lieu of training, MeSign maintains supporting documentation.

5.3.4 Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. MeSign makes all employees acting in trusted roles aware of any changes to MeSign' operations. If MeSign' operations change, MeSign will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

MeSign employees failing to comply with this CPS, whether through negligence or malicious intent, are Subject to administrative or disciplinary actions, including termination of employment or criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

No stipulation.

5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of this CPS, and other technical and operational documentation needed to maintain the integrity of MeSign' CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4 Audit Logging Procedures

5.4.1. Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

MeSign ensures all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. MeSign records the key operational events in the system, recorded events include but are not limited to the following:

1) CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2) CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists and OCSP entries.
3) Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;

e. Firewall and router activities; and

f. Entries to and exits from the CA facility.

Log entries include the following elements:

a. Date and time of entry;

b. Identity of the person making the journal entry; and

c. Description of the entry.

5.4.2. Frequency for Processing and Archiving Audit Logs

The MeSign internal auditor administrator reviews the system log at least once a month. And the audit logs are automatically archived in the system's database.

5.4.3. Retention Period for Audit Log

MeSign retains any audit logs generated for no less than ten (10) years, if required by law and makes these audit logs available to its Qualified Auditor upon request.

5.4.4. Protection of Audit Log

MeSign audit logs are digitally signed and stored in the database with backup, including audit information and event records in related documents. MeSign carries out strictly the measures of physical and logical access control to ensure that only personnel authorized by MeSign can be access to the records being reviewed. These records are strictly protected from unauthorized access, reading, modification and deletion, and the digitally signed with timestamped is for the technical guarantee of log temper-proof.

5.4.5. Audit Log Backup Procedures

Data is backed up daily in a rolling and increasing mode, including critical system data or any other sensitive information, like personal data and event log files. Archives and other materials of critical system data important for recovery in case of a disaster are stored in a secure manner at an off-site facility beyond 2,000 Kilometer of MeSign' main infrastructure.

5.4.6. Audit Collection System (Internal vs. External)

No stipulation.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

MeSign' Security Program includes regular risk assessments that:

1) Identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any data or processes.
2) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal data and certificate issuance processes.
3) Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that MeSign has in place to control such risks.

Based on the Risk Assessment, MeSign implements and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the data and processes, as well as the complexity and scope of the activities of MeSign.

The Security Plan includes administrative, organizational, technical and physical safeguards appropriate to the size, complexity, nature, and scope of the MeSign' business.
The Security Plan also takes into account the available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records Archival

5.5.1. Types of Records Archived

All accesses to the on-line and off-line systems and actions are logged as events including but not limited to remote IP addresses, identity, role, user agent, type of event, type of action, description, date and time. Security related events are additionally recorded with an issue tracking tool. Critical events are logged in a special report and signed by the CEO or COO of MeSign.

Records to be archived are those specified in Section 5.4.1.

5.5.2. Retention Period for Archive

MeSign retains the records of the issued certificates and the associated documentation for no less than ten (10) years. The retention term begins on the date of expiration or

revocation. Copies of certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that MeSign may see fit.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution or destruction.

5.5.4. Archive Backup Procedures

Same as 5.4.5

5.5.5. Requirements for Timestamping of Records

System times are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every day. All recorded events are time-stamped in the events and audit logs. Irrespective of timestamping methods, all logs must have data indicating the time at which the event occurred.

5.5.6. Archive Collection System (Internal or External)

Archive information is collected internally.

5.5.7. Procedures to Obtain and Verify Archive Information

Records are archived and maintained in a form that prevents unauthorized modification, substitution or destruction. Such records may be retained in electronic, in paper-based format or any other format that MeSign may see fit.

5.6 Key Changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, MeSign ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing Key Pair is commissioned, and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA Public Key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

In the event that a CA Private Key is suspected to have been compromised, MeSign' CEO or COO will immediately convene an emergency Incident Response Team to assess the situation to determine the degree and scope of the incident and take appropriate actions. Those include collection of information related to the incident, investigation, informing law enforcement and other interested parties, further prevention and short-term corrections, compiling and issuing of a critical events report. In case it was determined that a CA Private Key was compromised, the affected key shall be revoked (where possible) and a replacement issued after appropriate solutions are implemented to prevent recurrence.

MeSign maintains an Incident Response Plan and a Disaster Recovery Plan, which set out the procedures necessary to ensure business continuity, to notify affected stakeholders, and to reasonably protect Application Software, Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. MeSign annually tests, reviews, and updates its business continuity plan and its security plans and makes them available to the its auditors upon request.

The business continuity plan includes:
1). The conditions for activating the plan;
2). Emergency procedures;
3). Fallback procedures;
4). Resumption procedures;
5). A maintenance schedule for the plan;
6). Awareness and education requirements;
7). The responsibilities of the individuals;
8). Recovery time objective (RTO);
9). Regular testing of contingency plans;
10). A plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11). A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12). A definition of acceptable system outage and recovery times;
13). The frequency at which backup copies of essential business information and software are taken;
14). The distance of recovery facilities to the CA's main site; and
15). Procedures for securing an affected facility following a disaster and prior to restoring a secure environment either at the original or a remote site.

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

MeSign performs system back-ups on daily basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location. In the event of a disaster whereby the CA operations become inoperative, MeSign will re-initiate its operations on replacement hardware using backup copies of its software, data and CA Private Keys at a comparable, secured facility.

5.7.3. Recovery procedures after Key Compromise

In the event that the Root CA Private Key of MeSign is compromised, MeSign will:

- Immediately cease using the compromised key material;
- Revoke all Certificates signed with the compromised key;
- Take commercially reasonable steps to notify all Subscribers of the Revocation; and
- Take commercially reasonable steps to cause all Subscribers to cease using, for any purpose, any such Certificates.

Once the compromised key material has been replaced and a secure operation of the CA in question has been established, the CA may re-issue the revoked certificates following the procedure for initially providing the certificates.

5.7.4. Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1.

5.8 CA or RA Termination

In the event of termination of a MeSign CA, MeSign provides notice to all customers prior to the termination and:

1) Stops delivering Certificates according to and referring to this CPS;
2) Archives all audit logs and other records prior to termination;
3) Destroys all Private Keys upon termination;
4) Ensures archive records are transferred to an appropriate authority;
5) Uses secure means to notify customers and Application Software Suppliers to delete all trust anchors.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

MeSign Generates the Root CA key as required:

1) prepare and follow a Key Generation Script and
2) have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.
3) generate the keys in a physically secured environment as described in this CPS;
4) generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
5) generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CPS;
6) log its CA key generation activities; and
7) maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CPS and its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

MeSign provides Subscriber encryption certificate Private Key generation services, and Subscriber encryption certificate Private Keys must be generated within a secure cryptographic device that meets with FIPS 140-2 level 3. Such cryptographic devices perform subscriber key generation using a random number generator (RNG) or pseudo random number generator (PRNG) as specified in the ANSI X9 or ISO standard ISO/IEC 18032. When MeSign generates the keys, they may be generated on the following devices:

- Card/cryptographic token; or
- HSM device.

When subscriber generates the keys, they may be generated on the following devices;

- User browser certificate container;
- Web server key container;
- MeSign' secure container; and
- MeSign' application container for mobile phones.

6.1.2. Private Key Delivery to Subscriber

MeSign offers the creation of Key Pairs and certificate signing requests (CSR) for Client certificate (Encryption Certificate only) through the CA system. The Private Key is protected by a passphrase and delivered via SSL secured connection to the subscriber.

Subscribers may produce and prepare their own Private Keys and certificate signing requests (CSR) for server certificates and client certificates and submit them via SSL secured connection to CA system. In this case, Private Key delivery to the subscriber is unnecessary.

6.1.3. Public Key Delivery to Certificate Issuer

An issued certificate is either delivered through an on-line collection method or retrieved from the provided on-line interfaces. A subscriber is deemed to have accepted a certificate when delivered and installed into client or server software or when retrieved from the on-line interfaces.

6.1.4. CA Public Key Delivery to Relying Parties

The public Root CA keys and intermediate CA Public Keys are published from the following repository: https://www.mesign.com/root/
The public Root CA keys shall be embedded within popular software applications, making special root distribution mechanisms unnecessary.

6.1.5. Key Sizes

MeSign supports RSA key length of 2048 bits or more, supports ECC key length of 256 bits or more.

6.1.6. Public Key Parameters Generation and Quality Checking

MeSign generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission.

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

CA certificates include key usage extension fields to specify the purposes for which the CA Certificate may be used and also to technically limit the usage of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of MeSign. Key usages are specified in the Certificate Profile set forth in Section 7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The Private Keys of the Intermediate CA certificates are stored in Hardware Security Modules (HSM) FIPS 140-2 Level 3 certified devices, suitable for the signing of Subscriber Certificates and the online Certificate Revocation Lists. For recovery and archival purpose, the Private Keys of the Intermediate CA certificates are also cloned and stored off-line according to the same procedure as the CA root key.

The Encryption Certificate Private Key that MeSign APP uses, is generated in a Hardware Security Modules (HSM) device which is certified under FIPS 140-2 Level 3. Each of the Private Key is split into two parts, encrypted and stored into two separated Key Management Servers.

6.2.2. Private Key (n out of m) Multi-Person Control

MeSign' authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

Backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

MeSign does not escrow its signature keys. Subscribers may not escrow their private signature keys.

6.2.4. Private Key Backup

If required for business continuity MeSign backs up Private Keys under the same multi-person control as the original Private Key.

6.2.5. Private Key Archival

Private Keys belonging to MeSign are not archived by parties other than MeSign.

6.2.6. Private Key Transfer into or From a Cryptographic Module

All root keys must be generated by and in a cryptographic module. Private Keys can't be exported from the cryptographic module. For backup, use the same type HSM device to clone as backup HSM, the clone operation requires at least two-person access.

6.2.7. Private Key Storage on Cryptographic Module

MeSign stores Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8. Activating Private Key

MeSign' Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. See also Section 6.4.

6.2.9. Deactivating Private Key

MeSign' Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. Root Private Keys are further deactivated by removing them entirely from the storage partition on the HSM device. MeSign never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10. Destroying Private Key

MeSign personnel, acting in trusted roles, destroy CA Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.
MeSign may destroy a Private Key by deleting it from all known storage partitions. MeSign also zeroizes the HSM device according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, MeSign will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

6.2.11. Cryptographic Module Capabilities

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1. Public Key Archival

MeSign archives Public Keys from Certificates.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

All certificates and corresponding keys shall have maximum Validity Periods (not exceeding):

- Root CA 25 years
- Sub CA 10-15 years
- Subscriber Certificates: For client certificate, it has a Validity Period no greater than 39 months.

Pursuant to Section 5.6 CA Private Keys are retired from signing subordinate certificates before the periods listed above to accommodate the key changeover process (i.e., the retiring CA Private Key is still used to sign CRLs to provide validation services for certificates issued with that retiring CA Private Key.)

6.4 Activation Data

6.4.1. Activation Data Generation and Installation

MeSign activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. MeSign will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All MeSign personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. MeSign employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their password on a regular basis.

6.4.2. Activation Data Protection

MeSign protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All PIN codes and

USB key PINs are kept in sealed envelopes, which are placed in locked Safe Box and taken out by the CEO or CTO when used. MeSign locks accounts used to access secure CA processes if a certain number of failed password attempts occur.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

MeSign implements various access codes, smart cards, electronic tokens and physical locks in multiple combinations thereof for facility access, workstations, CA administration programs, server administration programs and monitoring devices to restrict and control access according to the defined roles and permissions.

6.5.2. Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1. System Development Controls

Development of the CA related infrastructures, hardware, libraries, programs, protective programs are performed by personnel with the appropriate knowledge and training.
Changes to configuration files and settings, sources, binaries and hardware components must be reviewed and approved by the management. Modifications to the processes and certificates are tested for eventual flaws. Maintenance and other activities on hardware the CA require prior approval by the management and are logged accordingly, monitored and recorded.

6.6.2. Security Management Controls

MeSign has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, MeSign can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by

management.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The CA root key(s) are kept off-line and brought online only when necessary to sign intermediate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

6.8 Time Stamping

All MeSign components are regularly synchronized with a reliable time service. MeSign operates a trusted Time-Stamping Authority (TSA) that compliant with RFC 3161. The TSA Certificate shall be in a FIPS 140-2 level 3 HSM. MeSign TSA provides RFC 3161-compliant timestamps and Authenticode Timestamp. The time stamping service is available at http://tsa.mesince.com.

For RFC 3161-compliant timestamps, MeSign includes a unique integer for each newly generated time - stamp token. MeSign only time - stamps hash representations of data, not the data itself. Information can be hashed for time - stamping using SHA-256 with RSA encryption and 2048-bit key size for signature creation. (SHA-1, SHA-256, SHA-384 and SHA-512 are supported for RFC 3161-based requests.) MeSign does not examine the imprint being time-stamped other than to check the imprint's length.
No warranty is offered, and no liability will be accepted for any use of the MeSign TSA which is made other than using a MeSign issued certificates, except contracted TSA users.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

MeSign Certificates conform to RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standards. In cases where stipulations of RFC 5280 and the applicable CA/Browser Forum Baseline Requirements differ, the Baseline Requirements notion will be adhered to.

MeSign generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate Extensions

MeSign issues Certificates in compliance with RFC 5280 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.2.1 Root CA Certificate

Duration: 25 years
Algorithm: SHA-256 or P-384 (ECC with sha-384)
Key size: 4096 bits or P-384
Serial number: non-sequential greater than zero and containing at least 64 bits of output from a CSPNRG

As per CABF BRs 7.1.2.1 and RFC 5280

- **basicConstraints:** MUST be present as critical extension. The CA field MUST be set to true. The pathLenConstraint field SHOULD NOT be present.
- **keyUsage:** MUST be present as critical extension. Bit positions for keyCertSign and cRLSign MUST be set.
- **certificatePolicies:** This extension SHOULD NOT be present.
- **extendedKeyUsage:** This extension MUST NOT be present.
- **Subject information:**
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- **organizationName (OID 2.5.4.10):** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

7.1.2.2 Subordinate CA Certificate

Duration: 10-15 years
Algorithm: SHA-256 or P-256 (ECC with sha-256)
Key size: 2048 bits or P-256
Serial number: non-sequential greater than zero and containing at least 64 bits of output from a CSPNRG

For Timestamp, as per Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates Appendix B Section (4)

- **cerificatePolicies**: This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints**: This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess**: this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP Responder.
- **basicConstraints**: This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.
- **keyUsage**: This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- **extKeyUsage**: The id-kp-timeStamping [RFC5280] value MUST be present. anyExtendedKeyUsage MUST NOT be present. Other values SHOULD NOT be present. This extension SHOULD be marked non-critical.
- **Subject information**:
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- **organizationName (OID 2.5.4.10):** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

For Client, as per RFC 5280

- **cerificatePolicies**: This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints**: This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **basicConstraints**: This extension MUST be present and MUST be marked critical. The CA field MUST be set true. The pathLenConstraint field MAY be present.
- **keyUsage**: This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- **extKeyUsage**: The emailProtection value MUST be present. anyExtendedKeyUsage , serverAuth , codeSigning , timeStamping MUST NOT be present.
- **Subject information**:
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

organizationName (OID 2.5.4.10): This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

7.1.2.3 Subscriber Certificate

Serial number: non-sequential greater than zero and containing at least 64 bits of output from a CSPNRG

For Timestamp certificate, as per RFC3161

- **certificatePolicies:** This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoint:** This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess:** this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP Responder and the HTTP URL for the Root CA's certificate
- **basicConstraints (optional):** The cA field MUST NOT be true.
- **keyUsage (required):** This extension MUST be present and MUST be marked critical. The bit positions for digitalSignature MUST be set. Bit positions for keyCertSign and cRLSign MUST NOT be set. All other bit positions SHOULD NOT be set.
- **extKeyUsage(required)**: The value id-kp-timeStamping [RFC5280] MUST be present and MUST be marked critical. The value anyExtendedKeyUsage MUST NOT be present.

For Client certificate, as per RFC 5280

- **cerificatePolicies:** This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints:** This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **basicConstraints (optional):** The CA field MUST NOT be true.
- **keyUsage(required)**: This extension MUST be present and MUST be marked critical. The bit positions for digitalSignature MUST be set.
- **extKeyUsage(required):** The emailProtection value MUST be present. anyExtendedKeyUsage , serverAuth , codeSigning , timeStamping MUST NOT be present.

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. MeSign does not issue a Certificate with:

- Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network).
- semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.3 Algorithm Object Identifiers

MeSign issues certificates using the following algorithm identifiers including SHA256WithRSA, SHA384WithRSA, ECDSAWithSH256, ECDSAWithSH384.

7.1.4 Name Forms

MeSign issues Certificates with name forms compliant to RFC 5280. Within the domain of each Issuing CA, MeSign includes a unique non-sequential Certificate serial number that exhibits at least 20 bits of entropy.

7.1.4.1 Issuer Information

MeSign Make sure that the contents of the Certificate Issuer Distinguished Name field match the Subject DN of the issuing CA.

7.1.4.2 Subject Information – Subscriber Certificates

By issuing the Certificate, MeSign represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

By issuing Root Certificate and a Subordinate CA Certificate, MeSign represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OID for MeSign is **1.3.6.1.4.1.50775**, MeSign issues certificates contain the following OIDs / OID arcs:

1) MeSign CPS version：
   1.3.6.1.4.1.50775.1.<major-version>.<minor-version>
2) MeSign special purpose OID：
   1.3.6.1.4.1.50775.2.<number>
   Adobe OID: 1.3.6.1.4.1.50775.2.9
   Email Validation Code OID: 1.3.6.1.4.1.50775.2.10

3) MeSign Intermediate root certificate (Issuer CA) OID：
   1.3.6.1.4.1.50775.3.<cert-type>
4) MeSign User certificate OID：
   1.3.6.1.4.1.50775.3.<cert-type>.<cert-class>
5) MeSign Validation Level OID：
   1.3.6.1.4.1.50775.11 V1 certificate
   1.3.6.1.4.1.50775.12 V2 certificate
   1.3.6.1.4.1.50775.13 V3 certificate
   1.3.6.1.4.1.50775.14 V4 certificate

Definition:
<cert-type>: 3: Client; 4: Timestamp; 5: PDF; 6: OCSP
<cert-class>: 1: V1; 2: V2; 3: V3; 4: V4

Digitally Signed Object	**Object Identifier (OID)**
Client Certificates Issuer CA	1.3.6.1.4.1.50775.3.3
Employee Identity Validation (V4) Client Certificates	1.3.6.1.4.1.50775.3.3.**4** 1.3.6.1.4.1.50775.2.9 (Adobe)
Organization Validation (V3) Client Certificates	1.3.6.1.4.1.50775.3.3.**3** 1.3.6.1.4.1.50775.2.9 (Adobe)
Individual Validation (V2) Client Certificates	1.3.6.1.4.1.50775.3.3.**2** 1.3.6.1.4.1.50775.2.9 (Adobe)
Email Validation (V1) Client Certificates	1.3.6.1.4.1.50775.3.3.**1**
Time Stamping Certificates Issuer CA	1.3.6.1.4.1.507753.4
Time Stamping Certificates	1.3.6.1.4.1.50775.3.4.**3**

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

MeSign certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

MeSign issues version 2 CRLs that contain the following fields:

- Version: v2
- Signature Algorithm: SHA256WithRSA
- Issuer: Identification of the CA issuing the CRL
- Last Update: Time of CRL issue
- Next Update: Time of next CRL issue (5 days)
- Revoked certificates: Listing of information for revoked certificates
- Revocation Date: Date of Revocation

7.2.2 CRL and CRL Entry Extensions

- Authority Key Identifier: Issuing CA Key Identifier
- CRL Number: a monotonically increasing sequence number.

7.3 OCSP Profile

7.3.1 Version Number(s)

Online Certificate Status Protocol responders conform to version 1 of RFC 2560.

7.3.2 OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

The practices specified in this CPS are designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

As part of its Security Program, MeSign controls its service quality each quarter by performing ongoing self-audits against a randomly selected sample of at least three percent (3%) of the V2/V3/V4 Certificates it has issued in the period beginning immediately after the last sample was taken.

8.1 Frequency and Circumstances of Assessment

An annual audit is or will be performed by an independent external auditor to assess MeSign' compliance with the AICPA/CICA WebTrust program for Certification Authorities and other related audit.

8.2 Identity/Qualifications of Assessor

MeSign' CA compliance audits are performed by WebTrust License Practitioners that:

1) Independence from the subject of the audit;
2) The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8.0 of this document;
3) Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4) Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
5) Bound by law, government regulation, or professional code of ethics.
6) Except in the case of an internal government auditing agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million ($1,000,000) US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

MeSign' WebTrust auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against MeSign.

8.4 Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following:

1) CA business practices disclosure,
2) Service integrity,
3) CA environmental controls,
4) CA key life cycle management, and
5) Certificate life cycle management.

8.5 Actions Taken as a Result of Deficiency

Upon detection of deficiencies and possible weaknesses of the CA infrastructure and/or established procedures as a result of internal or external auditing or in case of non-compliance

thereof, MeSign shall take corrective measures and actions in order to correct deficiencies and ensure future compliance within a reasonable time-frame. MeSign shall record, approve and report any corrective action steps taken and/or action steps that are anticipated to correct the non-compliant areas. The annual audit shall confirm the improvements and corrective measures taken.

8.6 Communications of Results

The results of each audit are reported to the MCPA and to any third-party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. On an annual basis, MeSign submits a report of its audit compliance to various parties if need. Such results shall be available no later than three (3) months after the end of the Audit Period. In the event of a delay greater than three months, MeSign shall provide an explanatory letter signed by the Qualified Auditor.

8.7 Self-Audits

MeSign monitors its adherence to this CPS by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. Other Business and Legal Matters

9.1 Fees

9.1.1. Certificate Issuance or Renewal Fees

MeSign charges Subscriber fees for some of the certificate services it offers, including issuance, renewal. Such fees are detailed on the official MeSign websites (www.mesign.com).

9.1.2. Certificate Access Fees

MeSign may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation or Status Information Access Fees

MeSign does not charge fees for the revocation of a certificate or for a Relying Party to check

the validity status of a MeSign issued certificate using Certificate Revocation Lists. MeSign retains its right to apply changes to such fees.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Subscribers must request refunds within 30 days after a Certificate issues. After receiving the refund request, MeSign may revoke the Certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

9.2 Financial Responsibility

9.2.1. Insurance Coverage

No stipulation.

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

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

1) Private Keys;
2) Activation data used to access Private Keys or to gain access to the CA system;
3) Business continuity, incident response, contingency, and disaster recovery plans;
4) Other security practices used to protect the confidentiality, integrity, or availability of information;
5) Information held by MeSign as private information in accordance with Section 9.4;

6) Audit logs and archive records; and
7) Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2. Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

MeSign' employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of Personal Information

9.4.1. Privacy Plan

MeSign respects the privacy of individuals and entities and shall not disclose personal details of certificate Applicants or other identifying information it retains from and about them to third parties.

9.4.2. Information Treated as Private

Any information about subscribers that is not publicly available through the content of the issued certificate, certificate directory and Certificate Revocation Lists, shall be treated as private and regarded as protected information.

9.4.3. Information Not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

Obtained private details and information shall not be used without the consent of the party to whom that information applies beyond the tasks MeSign has to perform for successful validation and verification purpose. MeSign shall save and secure subscriber information it retains from compromise and disclosure to third parties and shall comply with applicable local

privacy laws for the protection of such information.

9.4.5. Notice and Consent to Use Private Information

Personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. MeSign will only use private information after obtaining the Subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

If disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents, MeSign shall be entitled to disclose private information to law officials without penalty.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

Digital certificates which are the result of the operations of MeSign, are at any given time and remain during their whole lifetime the property of MeSign. Ownership of digital certificates issued by and through the operations of MeSign cannot be claimed by subscribers, relying parties, software vendors or any other party. Issuance of a certificate to the end user gives the subscriber the right to use the issued certificate(s), Subjected to the requirements and obligations set forth in this policy, acceptance of the terms and conditions of MeSign as published on the related web site(s) and to the extent of the key usage and extended key usage fields of the certificate, until expiration or revocation of the certificate, whichever comes first. MeSign exclusively retains the copyright of all certificates produced, created, published and issued by MeSign at all times and all rights are reserved.

9.6 Representations and Warranties

9.6.1. CA Representations and Warranties

MeSign uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. All parties including MeSign

and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been compromised, they will immediately notify MeSign.

MeSign represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid, MeSign has complied with its CPS in issuing and managing the Certificate:

- **Right to Use Domain Name or Email Address:** That, at the time of issuance, MeSign (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) or IP address(es) or email address listed in the Certificate's Subject field and Subject AltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in MeSign' CPS (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, MeSign (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in MeSign' CPS (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, MeSign (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the Subject: organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in MeSign' CPS (see Sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, MeSign (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's Subject: organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in MeSign' CPS (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, MeSign (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in MeSign' CPS (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if MeSign and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if MeSign and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);
- **Status:** That MeSign maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That MeSign will revoke the Certificate for any of the reasons specified in the Baseline Requirements and other guidelines as applicable (see Section 4.9.1).

9.6.2. RA Representations and Warranties

No stipulation.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify MeSign if a change occurs that could affect the status of the Certificate. Subscribers represent to MeSign, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

- **Accuracy of Information:** Subscriber will provide accurate and complete information at all times to MeSign, both in the Certificate Request and as otherwise requested by MeSign in connection with issuance of a Certificate;
- **Protection of Private Key:** Subscriber shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;
- **Acceptance of Certificate:** Subscriber shall review and verify the Certificate contents for accuracy;
- **Use of Certificate:** Subscriber shall install the SSL Certificate only on servers that are accessible at the Subject AltName(s) listed in the Certificate or shall install the S/MIME Certificate only for the email address at Subject AltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- **Reporting and Revocation:** Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- **Termination of Use of Certificate:** Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness:** Subscriber shall respond to MeSign' instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance:** MeSign is entitled to revoke the Certificate immediately if the Subscriber violates the terms of the Subscriber Agreement or Terms of Use or if MeSign discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a MeSign Certificate, it:

1) Obtained sufficient knowledge on the use of digital Certificates and PKI,
2) Studied the applicable limitations on the usage of Certificates and agrees to MeSign'

limitations on liability related to the use of Certificates,

3) Has read, understands, and agrees to the MeSign Relying Party Agreement and this CPS,
4) Verified both the MeSign Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,
5) Will not use a MeSign Certificate if the Certificate has expired or been revoked, and
6) Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a MeSign Certificate after considering:
   a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
   b) the intended use of the Certificate as listed in the certificate or this CPS,
   c) the data listed in the Certificate,
   d) the economic value of the transaction or communication,
   e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
   f) the Relying Party's previous course of dealing with the Subscriber,
   g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
   h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, MESIGN DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON‐INFRINGEMENT. MESIGN DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. MeSign does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an entity uses MeSign' services.

9.8 Limitations of Liability

MeSign gives no guaranties whatsoever about the security or suitability of the services

provided that are identified by a certificate issued by MeSign or the use of thereof, including but not limited to the use of its websites and programs or any other service offered currently or in the future. The certification services are operated according to the highest possible levels of security and to the highest industry standards, but without any warranty.

Relying parties have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a certificate, and as such are solely responsible for deciding whether or not to rely on such information, and therefore shall bear the legal consequences of their failure to perform the Relying Party Obligations outlined in this policy.

Under no circumstances, including negligence, shall MeSign or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this or other services, even if advised of the possibility of such damage.

9.9 Indemnities

9.9.1 Indemnification by MeSign

MeSign shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to a Certificate issued by MeSign, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to a Certificate issued by MeSign where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the online repository, and the software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify MeSign, its partners, and any Trusted Root entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the

Compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify MeSign, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1. Term

This CPS and any amendments to the CPS are effective when published to MeSign' online repository and remain in effect until replaced with a newer version.

9.10.2. Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

MeSign will communicate the conditions and effect of this CPS's termination via the MeSign Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the Certificate is revoked or expired, even if this CPS terminates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1. Procedure for Amendment

MeSign is responsible for determining the suitability of certificate policies illustrated within this document. MeSign is also responsible for determining the suitability of proposed changes to the policy and practice statements prior to the publication of an amended version.

Subscribers and relaying parties will not be notified of impending changes of the policy. The policy is legally binding from the moment of its publication.

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that the policy and practice statements are not amended and published without the prior authorization by the management of MeSign.

9.12.2. Notification Mechanism and Period

MeSign posts CPS revisions to its website. MeSign does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. Major changes affecting accredited Certificates are announced and approved by the accrediting agency prior to becoming effective. The MCPA is responsible for determining what constitutes a material change of the CPS.

9.12.3. Circumstances Under Which OID Must be Changed

The MCPA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute Resolution Provisions

Disputes arising in relation to certificates issued according to the related Guidelines as published by the CA/Browser Forum shall be treated according those guidelines and only to the extend and scope set forth by those guidelines. This may include different interpretation of applicable laws and the locality of jurisdiction. The parties may however agree to solve disputes under different applicable laws and jurisdiction.

9.14 Governing Law

Any party involved shall try to resolve all disputes that might arise in a spirit of cooperation without formal procedures. Any legal dispute which cannot be resolved without formal procedures shall take place in China or at a different location if the parties agree or are ordered to do so by law.

9.15 Compliance with Applicable Law

This CPS shall be subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous Provisions

9.16.1. Entire Agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.16.2. Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent by MeSign.

9.16.3. Severability

Interpretation of legal disputes arising from the operation of MeSign shall be treated according to the China legal system and laws.

If any term of this policy should be invalid under applicable laws, the affected term shall be replaced by the closest match according to applicable laws and the validity of the other terms should not be affected.

9.16.4. Enforcement (attorney's fees and waiver of rights)

MeSign may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. MeSign' failure to enforce a provision of this CPS does not waive MeSign' right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by MeSign.

9.16.5. Force Majeure

MeSign incurs no liability if it is prevented, forbidden or delayed from performing, or omits to perform, any act or requirement by reason of: any provision of any applicable law, regulation or order; civil, governmental or military authority; the failure of any electrical, communication or other system operated by any other party over which it has no control; fire, flood, or other emergency condition; strike; acts of terrorism or war; act of god; or other similar causes beyond its reasonable control and without its fault or negligence.

9.17 Other Provisions

No Stipulation.