

DigiCert

Certificate Policy



DigiCert, Inc.
Version 5.4
September 29, 20202
801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

TABLE OF CONTENTS

1. INTRODUCTION.....	6
1.1.OVERVIEW.....	6
1.2.DOCUMENT NAME AND IDENTIFICATION.....	7
1.3.PKI PARTICIPANTS.....	10
1.3.1. DigiCert Policy Authority and Certification Authorities	11
1.3.2. Registration Authorities.....	11
1.3.3. Subscribers.....	11
1.3.4. Relying Parties.....	12
1.3.5. Other Participants.....	12
1.4.CERTIFICATE USAGE	12
1.4.1. Appropriate Certificate Uses	12
1.4.1.1 Assurance Levels.....	12
1.4.2 Prohibited Certificate Uses.....	13
1.5.POLICY ADMINISTRATION	13
1.5.1. Organization Administering the Document.....	13
1.5.2 Contact Person	13
1.5.2.1 Revocation Reporting Contact Person	14
1.5.3 Person Determining CPS Suitability for the Policy.....	14
1.5.4 CP Approval Procedures	14
1.6 DEFINITIONS AND ACRONYMS	14
1.6.1 Definitions.....	14
1.6.2 Acronyms.....	15
1.6.3 References.....	Error! Bookmark not defined.
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	17
21 REPOSITORIES.....	17
22 PUBLICATION OF CERTIFICATION INFORMATION.....	17
Certificate.....	Error! Bookmark not defined.
23 TIME OR FREQUENCY OF PUBLICATION	17
24 ACCESS CONTROLS ON REPOSITORIES	17
3 IDENTIFICATION AND AUTHENTICATION	18
3.1 NAMING.....	18
3.1.1 Types of Names.....	18
3.1.2 Need for Names to be Meaningful	18
3.1.3 Anonymity or Pseudonymity of Subscribers	18
3.1.4 Rules for Interpreting Various Name Forms	18
3.1.5 Uniqueness of Names	18
3.1.6 Recognition, Authentication, and Role of Trademarks.....	19
3.2 INITIAL IDENTITY VALIDATION.....	19
3.2.1 Method to Prove Possession of Private Key.....	19
3.2.2 Authentication of Organization and Domain/Email Control	19
3.2.3 Authentication of Individual Identity	24
3.2.3.1 Authentication for Role-based Client Certificates.....	25
3.2.3.2 Authentication of Devices with Human	25
3.2.4 Non-verified Subscriber Information	25
3.2.5 Validation of Authority	26
3.2.6 Criteria for Interoperation	26
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	26
3.3.1 Identification and Authentication for Routine Re-key	26
3.3.2 Identification and Authentication for Re-key After Revocation	27
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	28
4.1 CERTIFICATE APPLICATION	28
4.1.1 Who Can Submit a Certificate Application.....	28
4.1.2 Enrollment Process and Responsibilities.....	28
4.2 CERTIFICATE APPLICATION PROCESSING.....	28
4.2.1 Performing Identification and Authentication Functions.....	28
4.2.2 Approval or Rejection of Certificate Applications	29
4.2.3 Time to Process Certificate Applications	29
4.3 CERTIFICATE ISSUANCE	29

4.3.1 CA Actions during Certificate Issuance	29
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate.....	29
4.4 CERTIFICATE ACCEPTANCE	29
4.4.1 Conduct Constituting Certificate Acceptance	29
4.4.2 Publication of the Certificate by the CA	29
4.4.3 Notification of Certificate Issuance by the CA to Other Entities	29
4.5 KEY PAIR AND CERTIFICATE USAGE.....	30
4.5.1 Subscriber Private Key and Certificate Usage.....	30
4.5.2 Relying Party Public Key and Certificate Usage.....	30
4.6 CERTIFICATE RENEWAL.....	30
4.6.1 Circumstance for Certificate Renewal	30
4.6.2 Who May Request Renewal	30
4.6.3 Processing Certificate Renewal Requests	30
4.6.4 Notification of New Certificate Issuance to Subscriber	31
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate.....	31
4.6.6 Publication of the Renewal Certificate by the CA.....	31
4.6.7 Notification of Certificate Issuance by the CA to Other Entities	31
4.7 CERTIFICATE RE-KEY	31
4.7.1 Circumstance for Certificate Rekey	31
4.7.2 Who May Request Certification of a New Public Key	31
4.7.3 Processing Certificate Rekey Requests	31
4.7.4 Notification of Certificate Rekey to Subscriber	31
4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate	31
4.7.6 Publication of the Rekeyed Certificate by the CA.....	31
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	31
4.8 CERTIFICATE MODIFICATION	32
4.8.1 Circumstance for Certificate Modification.....	32
4.8.2 Who May Request Certificate Modification.....	32
4.8.3 Processing Certificate Modification Requests.....	32
4.8.4 Notification of Certificate Modification to Subscriber	32
4.8.5 Conduct Constituting Acceptance of a Modified Certificate	32
4.8.6 Publication of the Modified Certificate by the CA.....	32
4.8.7 Notification of Certificate Modification by the CA to Other Entities	32
4.9 CERTIFICATE REVOCATION AND SUSPENSION.....	32
4.9.1 Circumstances for Revocation	32
4.9.2 Who Can Request Revocation	34
4.9.3 Procedure for Revocation Request.....	35
4.9.4 Revocation Request Grace Period	35
4.9.5 Time within which CA Must Process the Revocation Request	35
4.9.6 Revocation Checking Requirement for Relying Parties	36
4.9.7 CRL Issuance Frequency	36
4.9.8 Maximum Latency for CRLs.....	36
4.9.9 On-line Revocation/Status Checking Availability	36
4.9.10 On-line Revocation Checking Requirements	36
4.9.11 Other Forms of Revocation Advertisements Available	37
4.9.12 Special Requirements Related to Key Compromise.....	37
4.9.13 Circumstances for Suspension.....	37
4.9.14 Who Can Request Suspension.....	37
4.9.15 Procedure for Suspension Request.....	37
4.9.16 Limits on Suspension Period.....	38
4.10 CERTIFICATE STATUS SERVICES	38
4.10.1 Operational Characteristics	38
4.10.2 Service Availability	38
4.10.3 Optional Features.....	38
4.11 END OF SUBSCRIPTION	38
4.12 KEY ESCROW AND RECOVERY	38
4.12.1 Key Escrow and Recovery Policy Practices.....	38
4.12.2 Session Key Encapsulation and Recovery Policy and Practices.....	39
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	40
5.1. PHYSICAL CONTROLS.....	40
5.1.1. Site Location and Construction	40
5.1.2. Physical Access.....	40

5.1.3 Power and Air Conditioning	40
5.1.4 Water Exposures	40
5.1.5 Fire Prevention and Protection.....	40
5.1.6 Media Storage	41
5.1.7 Waste Disposal	41
5.1.8 Off-site Backup	41
5.1.9 Certificate Status Hosting, CMS and External RA Systems.....	41
5.2 PROCEDURAL CONTROLS.....	41
5.2.1 Trusted Roles	41
5.2.1.1 CA Administrators	41
5.2.1.3 System Administrator/ System Engineer (Operator)	41
5.2.1.4 Internal Auditor Role	41
5.2.1.5 RA Administrators	42
5.2.2 Number of Persons Required per Task.....	42
5.2.3 Identification and Authentication for each Role.....	42
5.2.4 Roles Requiring Separation of Duties.....	42
5.3 PERSONNEL CONTROLS.....	42
5.3.1 Qualifications, Experience, and Clearance Requirements.....	42
5.3.2 Background Check Procedures.....	42
5.3.3 Training Requirements.....	43
5.3.4 Retraining Frequency and Requirements.....	43
5.3.5 Job Rotation Frequency and Sequence.....	43
5.3.6 Sanctions for Unauthorized Actions.....	43
5.3.7 Independent Contractor Requirements.....	43
5.3.8 Documentation Supplied to Personnel	44
5.4 AUDIT LOGGING PROCEDURES	44
5.4.1 Types of Events Recorded	44
5.4.2 Frequency of Processing Log.....	44
5.4.3 Retention Period for Audit Log.....	45
5.4.4 Protection of Audit Log	45
5.4.5 Audit Log Backup Procedures.....	45
5.4.6 Audit Collection System (internal vs. external).....	45
5.4.7 Notification to Event-causing Subject.....	45
5.4.8 Vulnerability Assessments	45
5.5 RECORDS ARCHIVAL.....	45
5.5.1 Types of Records Archived.....	45
5.5.2 Retention Period for Archive.....	46
5.5.3 Protection of Archive.....	46
5.5.4 Archive Backup Procedures.....	46
5.5.5. Requirements for Time-stamping of Records.....	46
5.5.6 Archive Collection System (internal or external)	46
5.5.7 Procedures to Obtain and Verify Archive Information.....	46
5.6 KEY CHANGEOVER.....	47
5.7 COMPROMISE AND DISASTER RECOVERY.....	48
5.7.1 Incident and Compromise Handling Procedures.....	48
5.7.2 Computing Resources, Software, and/or Data Are Corrupted	48
5.7.3 Entity Private Key Compromise Procedures	48
5.7.4 Business Continuity Capabilities after a Disaster.....	48
5.8 CA OR RA TERMINATION	49
6. TECHNICAL SECURITY CONTROLS	50
6.1. KEY PAIR GENERATION AND INSTALLATION.....	50
6.1.1. Key Pair Generation	50
6.1.2 Private Key Delivery to Subscriber	50
6.1.3 Public Key Delivery to Certificate Issuer	51
6.1.4 CA Public Key Delivery to Relying Parties	51
6.1.5 Key Sizes	51
6.1.6 Public Key Parameters Generation and Quality Checking	51
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field).....	51
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	52
6.2.1 Cryptographic Module Standards and Controls.....	52
6.2.1.1 Custodial Subscriber Key Stores	53
6.2.2 Private Key (n out of m) Multi-person Control.....	53

6.2.3 Private Key Escrow.....	53
6.2.4 Private Key Backup.....	53
6.2.5 Private Key Archival.....	53
6.2.6 Private Key Transfer into or from a Cryptographic Module.....	53
6.2.7 Private Key Storage on Cryptographic Module.....	54
6.2.8 Method of Activating Private Key.....	54
6.2.9 Method of Deactivating Private Key.....	54
6.2.10 Method of Destroying Private Key.....	54
6.2.11 Cryptographic Module Rating.....	54
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	54
6.3.1 Public Key Archival.....	54
6.3.2 Certificate Operational Periods and Key Pair Usage Periods.....	55
6.4 ACTIVATION DATA.....	55
6.4.1 Activation Data Generation and Installation.....	55
6.4.2 Activation Data Protection.....	56
6.4.3 Other Aspects of Activation Data.....	56
6.5 COMPUTER SECURITY CONTROLS.....	56
6.5.1 Specific Computer Security Technical Requirements.....	56
6.5.2 Computer Security Rating.....	57
6.6 LIFE CYCLE TECHNICAL CONTROLS.....	57
6.6.1 System Development Controls.....	57
6.6.2 Security Management Controls.....	58
6.6.3 Life Cycle Security Controls.....	58
6.7 NETWORK SECURITY CONTROLS.....	58
6.8 TIME-STAMPING.....	58
7. CERTIFICATE, CRL, AND OCSP PROFILES.....	61
7.1 CERTIFICATE PROFILE.....	61
7.1.1 Version Number(s).....	61
7.1.2 Certificate Extensions.....	61
7.1.3 Algorithm Object Identifiers.....	61
7.1.4 Name Forms.....	63
7.1.5 Name Constraints.....	63
7.1.5.1 Name-Constrained serverAuth CAs.....	63
7.1.5.2 Name-Constrained emailProtection CAs.....	63
7.1.6 Certificate Policy Object Identifier.....	63
7.1.7 Usage of Policy Constraints Extension.....	64
7.1.8 Policy Qualifiers Syntax and Semantics.....	64
7.1.9 Processing Semantics for the Critical Certificate Policies Extension.....	64
7.2 CRL PROFILE.....	64
7.2.1 Version number(s).....	64
7.2.2 CRL and CRL Entry Extensions.....	64
7.3 OCSP PROFILE.....	64
7.3.1 Version Number(s).....	64
7.3.2 OCSP Extensions.....	64
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	65
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT.....	65
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR.....	65
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	65
8.4 TOPICS COVERED BY ASSESSMENT.....	65
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	65
8.6 COMMUNICATION OF RESULTS.....	65
8.7 SELF-AUDITS.....	66
9 OTHER BUSINESS AND LEGAL MATTERS.....	67
9.3 FEES.....	67
9.3.1 Certificate Issuance or Renewal Fees.....	67
9.3.2 Certificate Access Fees.....	67
9.3.3 Revocation or Status Information Access Fees.....	67
9.1.4 Fees for Other Services.....	67
9.1.5 Refund Policy.....	67
9.2 FINANCIAL RESPONSIBILITY.....	67
9.2.1 Insurance Coverage.....	67
9.2.2 Other Assets.....	67

9.2.3 Insurance or Warranty Coverage for End-Entities.....	67
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION	67
9.3.1 Scope of Confidential Information	67
9.3.2 Information Not Within the Scope of Confidential Information	67
9.3.3 Responsibility to Protect Confidential Information	68
9.4 PRIVACY OF PERSONAL INFORMATION	68
9.4.1 Privacy Plan	68
9.4.2 Information Treated as Private.....	68
9.4.3 Information Not Deemed Private	68
9.4.4 Responsibility to Protect Private Information.....	68
9.4.5 Notice and Consent to Use Private Information.....	68
9.4.6 Disclosure Pursuant to Judicial or Administrative Process.....	68
9.4.7 Other Information Disclosure Circumstances.....	68
9.5 INTELLECTUAL PROPERTY RIGHTS	68
9.5.1 Property Rights in Certificates and Revocation Information	68
9.5.2 Property Rights in the CP.....	68
9.5.3 Property Rights in Names.....	68
9.5.4 Property Rights in Keys and Key Material.....	69
9.5.5 Violation of Property Rights	69
9.6 REPRESENTATIONS AND WARRANTIES	69
9.6.1 CA Representations and Warranties.....	69
9.6.2 RA Representations and Warranties.....	69
9.6.3 Subscriber Representations and Warranties	69
9.6.4 Relying Party Representations and Warranties.....	70
9.6.5 Representations and Warranties of Other Participants.....	70
9.7 DISCLAIMERS OF WARRANTIES.....	70
9.8 LIMITATIONS OF LIABILITY	70
9.9 INDEMNITIES	70
9.9.1 Indemnification by an Issuer CA	70
9.9.2 Indemnification by Subscribers	70
9.9.3 Indemnification by Relying Parties	71
9.10 TERM AND TERMINATION	71
9.10.1 Term.....	71
9.10.2 Termination	71
9.10.3 Effect of Termination and Survival.....	71
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	71
9.12 AMENDMENTS	71
9.12.1 Procedure for Amendment.....	71
9.12.2 Notification Mechanism and Period	72
9.12.3 Circumstances under which OID Must Be Changed	72
9.13 DISPUTE RESOLUTION PROVISIONS.....	72
9.14 GOVERNING LAW	72
9.15 COMPLIANCE WITH APPLICABLE LAW	72
9.16 MISCELLANEOUS PROVISIONS	72
9.16.1 Entire Agreement	72
9.16.2 Assignment.....	72
9.16.3 Severability	72
9.16.4 Enforcement (attorneys' fees and waiver of rights)	73
9.16.5 Force Majeure	73
9.17 OTHER PROVISIONS.....	73

1. INTRODUCTION

1.1. OVERVIEW

This Certificate Policy (CP) defines the procedural and operational requirements that DigiCert requires entities to adhere to when issuing and managing digitally signed objects (digital Certificates and time-stamp tokens) within DigiCert's PKI, excluding participants in DigiCert's Private PKI services, which are not cross-certified or publicly trusted. Specific requirements regarding those Certificates are set forth in the individual agreements with the appropriate DigiCert customer and the DigiCert Private PKI CP/CPS available in the DigiCert legal repository listed in section 2.1.

DigiCert's Certificate and time-stamp policies are controlled by the DigiCert Policy Authority (DCPA) that determines how this CP applies to Certificate Authorities (CAs), Registration Authorities (RAs), Processing Centers, Affiliates, Subscribers, Relying Parties, and other PKI entities that interoperate with or within the DigiCert PKI. For ease of reference herein, all CAs and parties issuing Certificates in accordance with this CP (including DigiCert,) are hereafter referred to as "Issuer CAs."

This document specifies the policies DigiCert adopts to meet the current versions of the following policies, guidelines, and requirements

Name of Policy/Guideline/Requirement Standard	Location of Source Document/Language
The Adobe Approved Trust List Technical Requirements	https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf
the Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-document/
the CAB Forum Guidelines for Extended Validation Certificates ("EV Guidelines")	https://cabforum.org/extended-validation/
the CAB Forum Guidelines for the Issuance and Management of Code Signing Certificates	https://cabforum.org/baseline-requirements-code-signing/
the CAB Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Microsoft Trusted Root Store (Program Requirements)	https://docs.microsoft.com/en-us/security/trusted-root/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-

	US/about/governance/policies/security-group/certs/policy/
Mozilla CA/Forbidden or Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_program.html
360 Browser CA Policy	https://caprogram.360.cn/#strategy
Chromium Root Store Policy	https://www.chromium.org/Home/chromium-security/root-ca-policy

With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between this CP and the requirements and guidelines above, then the CAB Forum requirements and guidelines above take precedence. Time-stamping policies are in accordance with IETF RFC 3161.

This CP is only one of several documents that govern the DigiCert PKI. Other important documents include Certification Practice Statements, registration authority agreements and practice statements, subscriber agreements, relying party agreements, customer agreements, privacy policies, and memoranda of agreement. DigiCert 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.

CAs shall disclose all Cross Certificates that identify the CA as the Subject in the established trust relationship.

Depending on the class and type of certificate, Digital Certificates may be used by Subscribers to secure websites, digitally sign code or other content, digitally sign documents and/or e-mails. The person who ultimately receives a signed document or communication, or accesses a secured website is referred to as a relying party, i.e., those individuals are relying on the certificate and have to make a decision on whether to trust it. A Relying Party must rely on a certificate in terms of the relevant Relying Party Agreement included in the Certificate.

These participants and other parties are described in more detail in section 1.3 of this CP.

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

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certificate Policy and was approved for publication on 2 August 2010 by the DigiCert Policy Authority (DCPA). The following revisions have been made to the original document:

Date	Changes	Version
29-September-2020	Updates to include SC30, SC31 requirements and practices from the CABF.	5.4
16-July-2020	Modifications made in section 5 and correlating sections to describe security controls in accordance with external requirements and WebTrust audit criterion. Additional language added to section 1.4.2 about prohibiting certificate pinning and web PKI used for non-web applications.	5.3
22-May-2020	Minor editorial updates.	5.2
27-March-2020	Added modifications to include the Level 3 NIST LOA certificates in accordance with NIST 800-63-3 and updates for OV .onion guidelines. Modified table in section 6.3.2.	5.1

06-February-2020	Consolidated legacy Certificate Policies to include OID arcs into this policy (2.16.840.1.113733.1.7, 2.23.140.1.1, 1.3.6.1.4.1.14370, 1.3.6.1.4.1.14370.1, and 2.16.840.1.113733.1.7.48.). Updated the document to meet requirements of version 2.35 of the FBCA CP.	5.0
22-November-2019	Minor editorial changes throughout the document for consistency and accuracy	4.20
25-July-2019	Added AATL 2.0 reference to section 1.6.3 for continuity. Modifications added to section 3.2.2 for details about information source review. Added security policy reference	4.19
17-April-2019	Edited sections 3.1.6, 3.2.1, 6.1.3, and 7.1.4 to clarify naming and proof-of-possession requirements.	4.18
01-March-2019	Added Class 2 Authentication-Only OID, clarified Legacy OIDs, added reference to IP address validation from Baseline Requirements, and updated certificate validity table in section 6.3.2.	4.17
09-October-2018	Updates made to meet Mozilla Root Policy v.2.6.1 throughout the document. Changes to sections 4.9.1, 4.9.3, and 4.9.5 to include new CABF requirements from BallotSC6 for revocation timelines.	4.16
23-August-2018	Updates throughout for Adobe AATL 2.0 and FBCA CP versions 2.29-2.32, added Class 1-3 OIDs, removed unused definitions and references to EU Qualified Certificates, updated sections 3.2.2 and 3.2.3 regarding email validation, added language in section 6.1.1 to specify that DigiCert never creates key pairs for publicly trusted end-entity TLS Certificates.	4.15
25-January-2018	Added language based on the CAB Forum's Baseline Requirements, as indicated by Mozilla's Self-Assessment process	4.14
8-November-2017	Made edits to conform CP with CPS and to clarify provisions. Also added provision concerning the processing of CAA records.	4.13
8-September-2017	Removed references to PIV-I throughout, conflicts of interest in section 5.2.1, auditor qualifications in section 8.2, and made other minor changes.	4.12
23-February-2017	Updated address, made revisions related to the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and made other changes to update the CP.	4.11
9-September-2016	Updated to clarify ID documents allowed and for consistency with FBCA CP 2.29, and sec. 9.6.3 of Baseline Requirements	4.10
1-June-2015	Updated for consistency with CA/Browser Forum Baseline Requirements and new Federal PIV-I Profile reference	4.09
1-April-2015	Made additional changes based on FPKI CPWG review.	4.08
7-October-2014	Updated for consistency with FBCA CP v. 2.27	4.07
14-May-2014	Updated to comply with changes to Baseline Requirements and the EV Guidelines.	4.06
2-May-2013	Updated mailing address, removed references to Adobe CDS Program, revised explanation of Level 2 identification requirements, revised private key management provisions and key ceremony witness requirements.	4.05
10-May-2012	Updated to include provisions set forth in the Baseline Requirements, to add EV Code Signing, improve readability, and to modify requirements related to IGTF Certificates.	4.04

3-May-2011	Policy OIDs revised for certain certificate types and minor updates made to various sections.	4.03
29-October-2010	Changes made in response to comments from the FPKI CPWG regarding certificate status services, trusted roles, and off-site backup of archive.	4.02
26-August-2010	Updated the process used to authenticate the certificate requester's authority under section 3.2.5 for code signing certificates issued to organizations	4.01
2-August-2010	This version 4.0 replaces the DigiCert Certificate Policy and Certification Practices Statement, Version 3.08, dated May 29, 2009.	4.0

The OID for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412). DigiCert organizes its OID arcs for the various Certificates and documents described in this CP as follows:

Digitally Signed Object	Object Identifier (OID)
Policy Documents ¹	2.16.840.1.114412.0
This CP Document	2.16.840.1.114412.0.1.4
Certificates issued pursuant to CPS	2.16.840.1.114412.0.2.4
Non EV SSL/TLS Server Certificates	CABF B.R. OIDs required
Organization-Validated SSL/TLS Certificate	Required: 2.23.140.1.2.2 Optionally, or in legacy certificates: 2.16.840.1.114412.1.1
Domain-Validated SSL/TLS Certificate	Required: 2.23.140.1.2.1 Optionally, or in legacy certificates: 2.16.840.1.114412.1.2
Hotspot 2.0 OSU Server Certificates	2.16.840.1.114412.1.5
Extended Validation SSL/TLS Certificates per the EV SSL Guidelines	Required: 2.23.140.1.1 Optionally, or in legacy certificates: 2.16.840.1.114412.2.1 1.3.6.1.4.1.6334.1.100.1 (originally registered by beTRUSTed), and/or 2.16.840.1.113733.1.7.23.6 (originally registered by Verisign)
Object Signing Certificates	2.16.840.1.114412.3
Code Signing	2.16.840.1.114412.3.1
Code Signing per the Baseline Requirements for Code-Signing Certificates	Required: 2.23.140.1.4.1 Optionally, or in legacy Certificates: 2.16.840.1.114412.3.1.1
Extended Validation Code Signing per the Baseline Requirements for Code-Signing Certificates	Required: 2.23.140.1.3 Optionally, or in legacy Certificates: 2.16.840.1.114412.3.2
Windows Kernel Driver Signing	2.16.840.1.114412.3.11
Adobe Signing Certificates	2.16.840.1.114412.3.21
Client Certificate OID arc	2.16.840.1.114412.4.
Level 1 Certificates – Personal	2.16.840.1.114412.4.1.1 or 2.16.840.1.114412.5.1 (maps to 2.16.840.1.113733.1.7.23.1)
Level 1 Certificates – Enterprise	2.16.840.1.114412.4.1.2 or 2.16.840.1.114412.5.2 (maps to 2.16.840.1.113733.1.7.23.2)
Level 2 Certificates	2.16.840.1.114412.4.2 or 2.16.840.1.114412.5.2 (maps to 2.16.840.1.113733.1.7.23.1, 2.16.840.1.113733.1.7.23.2, or 2.16.840.1.113733.1.7.23.3)
Level 3 Certificates – Client	2.16.840.1.114412.4.3

Level 4 Certificates	2.16.840.1.114412.4.4.
Grid Certificates	2.16.840.1.114412.4.31 or 2.16.840.1.114412.31 (Grid-only arc)
IGTF-Comparable to Classic with Secured Infrastructure	2.16.840.1.114412.4.31.1 (Client w/ Public) or 2.16.840.1.114412.31.4.1.1 (Client Grid Only)
IGTF-Comparable to Member-Integrated Credential Services with Secured Infrastructure	2.16.840.1.114412.4.31.5
IGTF Grid Host – Public Trust	2.16.840.1.114412.1.31.1
Grid-Only Host Certificate	2.16.840.1.114412.31.1.1.1
Authentication-Only Certificates	2.16.840.1.114412.6
Class 2 Authentication-Only Certificates	2.16.840.1.114412.6.2
Legacy arc	2.16.840.1.114412.81
Test arc ¹	2.16.840.1.114412.99

Each OID above may be extended further to define additional policies covering a particular type of certificate. The extended OID shall be defined in the CPS for that product.

OIDs found in Certificates reliant upon CA/B Forum requirements and guidelines include the designated reserved policy identifiers in the Certificate Policy extension as of September 30, 2020. Certificates issued before that date include other OIDs that are designated in the table above as optional or specified as legacy due to being issued prior to the requirement date.

The following OID arcs are also included in this Policy, but are considered deprecated: 2.16.840.1.113733.1.7, 2.23.140.1.1, 1.3.6.1.4.1.14370, 1.3.6.1.4.1.14370.1, and 2.16.840.1.113733.1.7.48

This CP applies to any entity asserting one or more of the DigiCert OIDs identified above. When a CA issues a Certificate containing one of the above-specified policy identifiers, it asserts that the Certificate was issued and is managed in accordance with the requirements and responsibilities applicable to that respective policy and PKI participant. All other OIDs mentioned above belong to their respective owners, including those listed here:

Digitally Signed Object Owner and Name	Object Identifier (OID)
Certificate Authority and Browser Forum	
Domain Validated SSL/TLS Certificate	2.23.140.1.2.1
Organization Validated SSL/TLS Certificate	2.23.140.1.2.2
Individual Validated SSL/TLS Certificate	2.23.140.1.2.3
Extended Validated SSL/TLS Certificate	2.23.140.1.1
Extended Validated Code Signing Certificate	2.23.140.1.3
Microsoft	
Code Signing Certificate (for compliance with Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates)	2.23.140.1.4.1

Subsequent revisions to this CP might contain new OID assignments for the certificate types identified above.

1.3. ***PKI PARTICIPANTS***

¹ For Certificates that are no longer publicly-trusted, DigiCert utilizes the Legacy arc to clearly identify certificate chains requiring assistance with transitioning systems (e.g., older hardware and/or older algorithm use).

1.3.1. DigiCert Policy Authority and Certification Authorities

DigiCert Root Certificate Authorities and Intermediate CAs are managed by the DigiCert Policy Authority (DCPA) which is composed of members of DigiCert management appointed by DigiCert's executive management. The DCPA is responsible for this CP, the approval of related practice statements, and overseeing the conformance of CA practices with this CP. DigiCert's policies are designed to ensure that the DigiCert PKI complies, in all material respects, with U.S. and international standards and regulations, CA/Browser Forum Guidelines, and relevant law on electronic signatures.

DigiCert may establish or recognize other CAs (e.g. subordinate CAs) in accordance with this CP, applicable cross-certification / memoranda of agreement.

For ease of reference herein, all CAs issuing Certificates in accordance with this CP (including DigiCert) are hereafter referred to as "Issuer CAs."

1.3.2. Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate Applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of an Issuer CA on identity management systems (IdMs). DigiCert and subordinate Issuer CAs may act as RAs for certificates they issue. Entities that are not CAs are prohibited from performing any domain or IP address validation.

The requirements in this CP apply to all RAs. An Issuer CA shall monitor each RA's compliance with this policy, any other applicable CP, the applicable CPS, applicable external requirement documents listed in sections 1.1. and 1.6.3 of this CP, and if applicable, any Registration Practices Statement (RPS) under which the RA operates.

An Issuer CA that relies on a variety of RAs or IdMs to support various communities of interest may submit an RPS for each RA or IdM to the DCPA for approval. The RPS must contain details necessary for the DCPA to determine how the RA achieves compliance with this Policy. Necessary details include how the RA's process or IdM establishes the identities of applicants, how the integrity and authenticity of such identifying information is securely maintained and managed, and how changes and updates to such information are communicated to the Issuer CA.

1.3.3. Subscribers

Subscribers use DigiCert's services and PKI to support transactions and communications. Subscribers under this CP include all end users (including entities) of certificates issued by an Issuer CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the Certificate. A *Subscriber*, as used herein, refers to both the subject of the Certificate and the entity that contracted with the Issuer CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

CAs are technically also subscribers of certificates within the DigiCert Public PKI, either as the primary

Certificate Authority issuing a self- signed Certificate to itself, or as an Issuer CA issued a Certificate by a superior CA. References to “end entities” and “subscribers” in this CP, however, apply only to end-user Subscribers.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by the Issuer CA. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. A Relying party may also be a Subscriber of the DigiCert Public PKI hierarchy.

1.3.5. Other Participants

Other participants include Bridge CAs and CAs that cross-certify Issuer CAs to provide trust among other PKI communities.

1.4. CERTIFICATE USAGE

A *digital Certificate* (or *Certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

A *time-stamp token (TST)* cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non- verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. It is not the intent of this CP to limit the types of usages for Organizational Certificates. While an organizational certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

1.4.1. Appropriate Certificate Uses

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CP.

1.4.1.1 Assurance Levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity.

DV Certificates are issued to domains to provide encryption. Section 3.2.2 of the DigiCert CPS explains how DigiCert validates that the person enrolling for the certificate has control of the domain. No organization authentication is performed on the owner of the domain listed in a DV certificate.

High assurance Certificates are individual and organizational Certificates that provide a high level or class of assurance of the identity of the Subscriber in comparison with lower assurance level or class certificates.

High assurance with extended validation certificates are certificates issued by DigiCert in conformance with the Guidelines for Extended Validation Certificates.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued. Code signing Certificates do not indicate that the signed code is safe to install or is free from malware, bugs, or vulnerabilities.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

CA Certificates subject to the Mozilla Root Store Policy may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

Participants in the DigiCert Public PKI periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. DigiCert therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.

DigiCert strongly discourages key pinning and shall not consider it a sufficient reason to delay revocation. DigiCert continually researches and implements technological processes in order to detect pinned applications and other prohibited uses so we can counsel customers on the way pinning impacts the agility of the WebPKI (e.g., rotation of intermediate certificates). Customers should also take care in not mixing certificates trusted for the web with non-web PKI. Any certificates trusted by the browsers must comply with all requirements of all applicable browser root policies, including revocation periods of 24 hours and 5 days as asserted in the relevant policies, obligations, and requirements of this CP and the CPS.

1.5. *POLICY ADMINISTRATION*

1.5.1. Organization Administering the Document

This CP and the relevant documents referenced herein are maintained by the DCPA, which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600
Fax: 1-801-705-0481
support@digicert.com

1.5.2 Contact Person

Attn: Legal Counsel
DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way

Lehi, UT 84043 USA
www.digicert.com
support@digicert.com

1.5.2.1 Revocation Reporting Contact Person

Attn: Support
DigiCert Technical Support
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
revoke@digicert.com

For anyone listed in section 4.9.2 of this CP and the CA/Browser Baseline Requirements that needs assistance with revocation or an investigative report, DigiCert provides this page for reporting and submitting requests: <https://www.digicert.com/certificate-revocation.htm>

Specifics of how each individual Issuing CA accepts revocation requests must be detailed in the applicable CPS.

1.5.3 Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CP and the conformance of a CPS to this CP based on the results and recommendations received from an independent auditor (see Section 8). The DCPA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4 CP Approval Procedures

The DCPA approves the CP and any amendments. Amendments are made by either updating the entire CP or by publishing an addendum. The DCPA determines whether an amendment to this CP requires notice or an OID change. *See also* Section 9.10 and Section 9.12 below.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

“Affiliated Organization” means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a Certificate.

“Applicant” means an entity applying for a certificate.

“Base Domain Name” is as defined in the Baseline Requirements.

“Certificate” means an electronic document that uses a digital signature to bind a Public Key and an identity.

“Domain Name” is as defined in the Baseline Requirements.

“Domain Namespace” is as defined in the Baseline Requirements.

“EV Guidelines” is defined in section 1.1.

“Key Pair” means a Private Key and its associated Public Key.

“OCSP Responder” means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

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

“Relying Party” means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

“Relying Party Agreement” means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert’s Repository.

“Subscriber” means either the entity identified as the subject in the Certificate or the entity receiving DigiCert’s time-stamping services.

“Subscriber Agreement” means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

“WebTrust” means the current version of CPA Canada’s WebTrust Program(s) for Certification Authorities.

1.6.2 Acronyms

CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	CA/Browser as in “CAB Forum”
CBP	Commercial Best Practices
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DCPA	DigiCert Policy Authority
DV	Domain Validated
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PIN	Personal Identification Number (e.g. a secret access code)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SHA	Secure Hashing Algorithm

SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3 References

If not listed in section 1.1:

Adobe Approved Trust List Technical Requirements, v.2.0

CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”)

CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (“EV Guidelines”)

CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Code Signing Certificates

Wi-Fi Alliance Hotspot 2.0 Release 2 Online Signup Certificate Policy Specification (Hotspot 2.0 CP)

Mozilla Root Store Policy, v.2.7

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Issuer CAs shall publish all publicly trusted CA Certificates and cross-Certificates, issued to and from the Issuer CA, revocation data for issued digital Certificates, CP, CPS, and standard Relying Party Agreements and Subscriber Agreements in online repositories. The Issuer CA shall ensure that its root Certificate and the revocation data for issued Certificates are regularly available through an online repository.

The Issuer CA shall develop, implement, enforce, and annually update the CP and/or CPS to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. These updates also describe in detail how the CA implements the latest version of the Baseline Requirements.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Issuer CAs shall make the following information publicly accessible on the web: all publicly trusted root Certificates, cross Certificates, CRLs, CPs, and CPSs. Pointers to repository information in CA and end entity Certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

As specified in section 1.1, this CP and all CPS must be structured in accordance with RFC 3647 and include all material required by RFC 3647.

2.3 TIME OR FREQUENCY OF PUBLICATION

Issuer CAs shall publish CA Certificates and revocation data as soon as possible after issuance. Issuer CAs shall publish new or modified versions CPSs within seven days of their approval.

CRLs for end-user Subscriber Certificates containing a CRL distribution point shall be issued at least once every seven days. CRLs for CAs that only issue CA Certificates shall be issued at least annually, and also whenever a CA Certificate is revoked. CRLs for Authenticated Content Signing (ACS) Root CAs are published annually and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration.

If applicable based on the types of certificates they issue and the scope of the CA/Browser Forum Baseline Requirements, Issuer CAs shall develop, implement, enforce, and annually update a Certification Practices Statement that describes in detail how the CA implements the latest version of the CA/Browser Forum Baseline Requirements. Those updates indicate conformance by incrementing the version number and adding a dated changelog entry even if no other changes are made to the document as specified in section 1.2 of this CP.

2.4 ACCESS CONTROLS ON REPOSITORIES

Information published in a repository is public information. The Issuer CA shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

Issuer CAs shall issue Certificates with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. Level 1 Certificates may include a null subject DN if they include at least one alternative name form that is marked critical. Subject Alternate Name forms may be included in Certificates if they are marked non-critical. When DNs are used, common names must respect name space uniqueness and must not be misleading. Other attributes may be present within the subject field. If present, other attributes must contain information that has been verified by the CA or RA.

3.1.2. Need for Names to be Meaningful

When applicable, Issuer CAs shall use distinguished names to 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. Directory information trees shall accurately reflect organizational structures.

When applicable, Issuer CAs shall ensure that each User Principal Name (UPN) is unique and accurately reflects organizational structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Issuer CAs may issue end-entity anonymous or pseudonymous Certificates provided that (i) such Certificates are not prohibited by applicable policy (e.g. for certificate type, assurance level, or certificate profile) and (ii) name space uniqueness is preserved.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate shall be enforced as follows:

SSL/TLS Server Certificates	Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).
Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.
Document Signing Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.
IGTF and Grid-only Device Certificates	For device Certificates, an FQDN is included in the appropriate fields. For other Certificates, DigiCert may append a unique ID to a name listed in the Certificate.
Code Signing Certificates (including CDS Certificates)	Requiring a unique organization name and address or a unique organization name combined/associated with a unique serial integer.
Time Stamping	Requiring a unique hash and time or unique serial number assigned to the time stamp

The names of Subscribers shall be unique within a subordinate Issuer CA's and Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6. Recognition, Authentication, and Role of Trademarks

For publicly-trusted TLS/SSL, Issuer CAs shall implement a process that limits inclusion of an OU attribute that is a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with the EV Guidelines, Baseline Requirements, and section 3.2 of this CP and described in their respective CPS. For all other Certificates, unless otherwise specifically stated, this CP does not require an Issuer CA to verify an Applicant's right to use a trademark. Issuer CAs may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 INITIAL IDENTITY VALIDATION

An Issuer CA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The Issuer CA may refuse to issue a Certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organization and Domain/Email Control

An Issuer CA must take reasonable measures to verify that the entity submitting the request for a Certificate to be used to sign or encrypt email, controls the email account associated with the email address referenced in the Certificate, or was authorized by the email account holder to act on the account holder's behalf.

Issuer CAs and RAs shall check the accuracy of information sources and databases to ensure the data is considered accurate, including reviewing the database provider's terms of use.

Domain names included in a publicly trusted SSL/TLS Certificate must be verified in accordance with Section 3.2.2.4 of the Baseline Requirements.

IP Addresses included in a publicly trusted SSL/TLS Certificate must be verified in accordance with Section 3.2.5 of the Baseline Requirements.

If a publicly-trusted SSL/TLS Certificate will contain an organization's name, then the Issuer CA (or an RA) shall verify the information about the organization and its legal existence in accordance with Section 3.2.2.1 of the Baseline Requirements using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition.

If the request is for a Certificate that asserts an organizational affiliation between a human subscriber and an organization, the Issuer CA shall obtain documentation from the organization that recognizes the affiliation and obligates the organization to request revocation of the Certificate if that affiliation ends. See Sections 3.2.5, 4.9.1 and 9.6.1.

Issuer CAs issuing publicly-trusted EV SSL certificates shall disclose their verification sources in accordance with section 11.1.3 of the EV SSL Guidelines.

If the FQDN contains a wildcard character, then the Issuer 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.

Before issuing a certificate with a wildcard character in a CN or subjectAltName of a type DNS-ID, the CA must follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, the Issuer CA must refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace.

Issuer CAs must complete all Domain/IP Address validation procedures for TLS certificates—such validation procedures must not be completed by third parties.

Issuer CAs shall not delegate validation of the domain portion of an e-mail address in s/MIME certificates. The Issuer CA may rely upon validation the root CA has performed for an Authorized Domain Name as being valid domain names. If the Issuer CA is verifying the domain portion, then the Issuer CA must clearly specify in their applicable CPS how domains are verified, typically using a process the CA/B Forum authorized to meet this requirement.

For a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the Issuer CA confirms, as of the date the Certificate was issued, the Applicant’s control over the .onion Domain Name in accordance with Appendix F of the EV Guidelines or Appendix C of the Baseline Requirements when the FQDN contains “onion” as the rightmost label.

Certificate	Identity Verification
SSL/TLS Server Certificates and Object Signing Certificates (issued to an Individual)	The Applicant shall submit a legible copy, which discernibly shows the Applicant’s face, of at least one currently valid government- issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The copy of the document shall be inspected for any indication of alteration or falsification. For Object Signing Certificates, the Issuer CA or RA shall obtain a face-to-face identification of the Applicant (i.e. a Declaration of Identity), which may be performed via a video conference call. If the Issuer CA or RA requires further assurance, the Applicant shall provide additional forms of identification, including non- photo and non-governmental forms of identification such as recent utility bills, financial account statements, Applicant credit card, additional ID credential, or equivalent document type. The Issuer CA or RA shall confirm that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If the Issuer CA or RA cannot verify the Applicant’s identity using the procedures described above, then the Issuer CA or RA shall obtain a Declaration of Identity witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Device Certificate Sponsors	See section 3.2.3.3
EV SSL/TLS Certificates issued to a Business Entity	As specified in the EV Guidelines

Authentication-Only Certificates	The entity controlling the secure location represents that the certificate holder has authorization to access the location.
Grid-only Certificates	Either the RA responsible for the grid community or a Trusted Agent must either review an identity document during a face-to-face meeting with the Applicant, or a Trusted Agent must attest that the Applicant is personally known to the Trusted Agent. If an identification document is used, the RA must retain sufficient information about the Applicant's identity in order to verify the Applicant at a later date.
Level 1 Client Certificates – Personal (email certificates)	Applicant's control over an email address (or any of the identity verification methods listed for a higher level client certificate) as specified in section 3.2.2.
Level 1 Client Certificates – Enterprise (email certificates) ²	Any one of the following: 1. In-person appearance before an RA or Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: - the ability to place or receive calls from a given number; or - the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: - the ability to obtain mail at the billing address used in the business relationship; or - verification of information established in previous transactions (e.g., previous order number); or - the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method required to verify identity for issuance of a Level 2, 3, or 4 Client Certificate

² For Adobe Certificates, the required face to face validation procedures and other validation requirements are performed by a contracted RA with DigiCert as allowed.

Level 2 Client Certificates	This level of assurance requires that the Issuer CA or RA verify the Applicant's identity using the possession of a reliable form of identification. Personal identifying information shall be compared with Applicant-provided information to confirm that the asserted name matches: (a) the name contained in the presented identification credential; (b) the individual's date of birth; and (c) a current address or personal telephone number sufficient to identify a unique individual. The Issuer CA or RA shall verify the Applicant's identity using one of the following four (4) methods: 1. In-person proofing before an RA or Trusted Agent (or entity certified by a State or National Government as authorized to confirm identities) with presentment of a valid current government-issued identity document that contains the Applicant's picture and either address of record or nationality (e.g. driver's license or Passport). Such authentication does not relieve the RA of its responsibility to verify the presented data. 2. Remotely verifying information provided by the Applicant (verified electronically by a record check with the specified issuing authority or through similar databases to establish the existence of such records with matching name and reference numbers and to corroborate date of birth and current address of record or telephone number).
	The Issuer CA or RA may confirm an address by issuing the credentials in a manner that confirms the address of record or verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records that are available to the Issuer CA or RA. 3. If the Issuer CA or RA has a current, ongoing relationship with the Applicant, the Issuer CA or RA may verify identity using an exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo ID, and (b) the ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods required to verify identity for issuance of a DigiCert Level 3 or 4 Client Certificate.

Level 3 Client Certificates	In-person proofing³ before an RA, Trusted Agent, or an entity certified by a State or National Government that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). The Applicant shall provide at least one Federal Government-issued Picture I.D., a REAL ID, or two Non-Federal Government I.D.s, one of which must be a photo I.D. Acceptable forms of Non-Federal Government photo IDs include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See USCIS Form I-9. The Issuer CA or RA shall examine the credentials and determine whether they are authentic and unexpired. The Issuer CA or RA shall check the provided information (name, date of birth, and current address) to ensure legitimacy and may verify it electronically by a record
	check as described above. The Issuer CA or RA may employ an in-person antecedent process= to meet the in-person identity proofing requirement. Historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, the Applicant (e.g. an employee) has been identified previously by an employer using USCIS Form I-9 and is bound to the asserted identity remotely through the use of known attributes or shared secrets. If the photo ID is unexpired and confirms the address of record for the Applicant, then the certificate may be approved for issuance with notice of issuance sent to the address of record. If the photo ID does not confirm the Applicant's address of record, then the certificate shall be issued in a manner that confirms the address of record. For all Level 3 or higher assurance Client Certificates, the identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance. If the photo ID is unexpired and confirms the address of record for the Applicant, then the certificate may be approved for issuance with notice of issuance sent to the address of record. If the photo ID does not confirm the Applicant's address of record, then the certificate shall be issued in a manner that confirms the address of record. For all Level 3 or higher assurance Client Certificates, the identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.

Level 4 Client Certificates (Medium Hardware) ³	In-person proofing before an RA, Trusted Agent, or an entity certified by a State or National Government that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). The Application shall supply (i) one Federal Government-issued Picture I.D., a REAL ID, or two Non-Federal Government I.D.s, one of which must be a photo I.D. and (ii) the contemporaneous collection of at least one biometric (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application. Acceptable forms of Non-Federal Government photo IDs include a driver's license, state- issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See USCIS Form I-9.
	The Issuer CA or RA shall examine the credentials and determine whether they are authentic and unexpired. For all Level 4 Client Certificates the use of an in-person antecedent is not applicable and the Applicant shall establish his or her identity no more than 30 days prior to initial certificate issuance. Issuer CAs and RAs shall issue Level 4 Client Certificates in a manner that confirms the Applicant's address of record.

Issuer CAs and RAs shall identify high-risk certificate requests and shall conduct additional verification activity and take additional precautions as are reasonably necessary to ensure that high-risk requests are properly verified.

Issuer CAs are required to perform checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science ("BIS").

3.2.3 Authentication of Individual Identity

The Issuer CA or an RA shall verify an individual's identity in accordance with the process established in its CPS or RPS that meets the following minimum requirements:

Where in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate at the same or higher level of assurance applied for by the Applicant. The person accompanying the Applicant (i.e. the "Sponsor") will present information sufficient for registration at the level of the certificate being requested, for himself or herself, and for the Applicant.

For in-person identity proofing at Levels 3 and 4, an entity certified by a State or National Government as authorized to confirm identities may perform in-person authentication on behalf of

³ Must be issued to cryptographic hardware.

the RA. The information collected from the applicant should be reliably collected from the certified entity. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

3.2.3.1 *Authentication for Role-based Client Certificates*

An Issuer CA may issue Certificates that identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). These role-based Certificates are used when non-repudiation is desired. The Issuer CA may only issue role-based certificates to Subscribers who first obtain an individual Subscriber Certificate that is at the same or higher assurance level as the requested role-based Certificate. An Issuer CA may issue Certificates with the same role to multiple Subscribers. However, the Issuer CA shall require that each Certificate have a unique Key Pair. Individuals may not share their issued role-based Certificates and are required to protect the role-based Certificate in the same manner as individual Certificates.

The Issuer CA or an RA shall verify the identity of the individual requesting a role-based Certificate (i.e. the sponsor) in accordance with Section 3.2.3 and record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role-based Certificate. The sponsor must hold an individual Certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based Certificate.

Procedures and policies for issuing role-based Certificates shall comply with all provisions of this CP (e.g., key generation, private key protection, and Subscriber obligations).

IGTF Certificates are not issued as role-based Certificates.

3.2.3.2 *Authentication of Devices with Human*

An Issuer CA may issue a Level 1, 2, 3 or 4 Client Certificate for use on a computing or network device, provided that the entity owning the device is listed as the subject. In such cases, the device must have a human sponsor who provides:

Equipment identification (e.g., serial number) or service name (e.g., DNS name),
Equipment Public Keys,
Equipment authorizations and attributes (if any are to be included in the certificate), and
Contact information.

If the Certificate's sponsor changes, the new sponsor shall review the status of each device to ensure it is still authorized to receive Certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The Issuer CA shall verify all registration information commensurate with the requested certificate type. Acceptable methods for performing this authentication and integrity checking include:

1. Verification of digitally signed messages sent from the sponsor (using Certificates of equivalent or greater assurance than that being requested)
2. In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.

3.2.4 Non-verified Subscriber Information

Issuer CAs are not required to confirm that the common name in a Level 1 - Personal Client Certificate the legal name of the Subscriber. A trusted agent may be used to verify identity information where allowed. No unverified information shall be included in any Level 2, Level 3, Level 4, Object Signing, or EV Certificate.

TLS OU information shall be verified in accordance with section 3.2 if used. For other Certificate output the Organization Unit (OU) is not usually verified. The Issuing CA MUST follow a process for verifying that the OU does not contain an unverified name, trademark, or address.

3.2.5 Validation of Authority

The Issuer CA or RA shall verify the authorization of a certificate request as follows:

Certificate	Verification
DV SSL/TLS Certificates and OV SSL/TLS Certificates	An authorized contact listed with the Domain Name Registrar, a person with control over the domain name, or through communication with the applicant using a Reliable Method of Communication, as defined in the Baseline Requirements.
EV Certificates	In accordance with the EV Guidelines.
Object Signing Certificates (including EV Code Signing Certificates)	If a Certificate names an organization, an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a Reliable Method of Communication.
Level 1 Client Certificates - Personal or Enterprise (email certificates) issued through the native DigiCert infrastructure	An individual with control over the email address listed in the Certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the Certificate.
IGTF Certificates	Pursuant to the relevant requirements by the accreditation authority.
Client Certificates Levels 2, 3 and 4	Individuals affiliated with the organization who confirm the applicant's authority to obtain a Certificate indicating the affiliation and who agree to request revocation of the Certificate when that affiliation ends.

The Issuer CA shall implement a process whereby an Applicant may limit the number of individuals authorized to request Certificates. The Issuer CA shall provide a list of authorized certificate requesters after receiving a verified request for such information from an individual authorized to make such request.

3.2.6 Criteria for Interoperation

DigiCert may provide interoperation services that allow another CA to be able to interoperate by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with this CP as supplemented by additional policies when required.

DigiCert permits interoperation with another CA in circumstances where the CA:

- Enters into a contractual agreement with DigiCert;
- Operates under a CPS that meets requirements for the certificates it will issue;
- Passes a compliance assessment before being allowed to interoperate; and
- Passes an annual compliance assessment for ongoing eligibility to interoperate that meets the requirements of the program and section 8 of this CP.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

The entity representing the Subscriber approving a Certificate Application is responsible for authenticating a request for re-key or renewal. Re-key procedures ensure that the person or organization seeking to renew/rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

An Issuer CA may allow Subscribers of SSL/TLS Server and Code Signing Certificates to authenticate themselves over a TLS/SSL session with username and password. Each Subscriber shall reestablish its identity using the initial registration processes of section 3.2 according to the following table:

Certificate	Routine Re-Key Authentication	Re-Verification Required
DV and OV SSL/TLS Certificates	Username and password	According to the Baseline Requirements
EV SSL/TLS Certificates	Username and password	According to the EV Guidelines
Subscriber Code Signing Certificates (Minimum Requirements and EV)	Username and password	According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
Signing Authority EV Code Signing Certificates	Username and password	According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
Timestamp EV Code Signing Certificates	Username and password	According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
Object Signing Certificates	Username and password	At least every six years
Level 1 Client Certificates	Username and password or a challenge phrase	At least every nine years
Level 2 Client Certificates and AATL certs	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3 or a challenge phrase	At least every nine years
Level 3 and 4 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
IGTF Certificates	Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated Private Key	At least every 13 months. However, certificates associated with a Private Key restricted solely to a hardware token may be rekeyed or renewed for a period of up to 5 years
Authentication-Only Certificates	Username and password or with associated Private Key	None

3.3.2 Identification and Authentication for Re-key After Revocation

The Issuer CA shall require subscribers of Certificates to undergo the initial registration process (described in Section 3.2) to obtain a new Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The Issuer CA or the RA that approved the Certificate's issuance shall authenticate all revocation requests. The Issuer CA or RA may authenticate a revocation request using the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate;
- Any authorized representative of an Organization or entity;
- Any authorized representative of an Issuer CA; or
- Any authorized representative of an RA.

No individual or entity listed on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the United States may submit an application for a Certificate. Applicants or individuals authorized to request Certificates, who are not included in any of the previous lists, may apply for a Certificate.

4.1.2 Enrollment Process and Responsibilities

The Issuer CA is responsible for ensuring that the identity of each Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of any Certificate type per the applicable legal agreements. Applicants are responsible for submitting sufficient information and documentation for the Issuer CA or the RA to perform the required verification of identity prior to issuing a Certificate.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

The Issuer CA or RA shall identify and verify each Applicant in accordance with the applicable Certification Practices Statements and Registration Practices Statements. In cases where the certificate request does not contain all the necessary information about the Applicant, Issuer CAs shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. Issuer CAs and its RAs shall follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

An Issuer CA issuing publicly trusted SSL/TLS server certificates shall state in its CPS its practices on processing CAA Records for Fully Qualified Domain Names. As of September 8, 2017, the Issuer CA for TLS certificates must check the CAA issue and issuewild records within 8 hours of issuance or the CAA record's Time to Live (TTL), whichever is greater, except where CAA was similarly checked prior to the creation of a Certificate Transparency pre-certificate that was logged in at least 2 public CT log servers. CAA checking may be omitted for technically- constrained subordinate CAs.

DNS access failure can be treated as permission to issue when the failure is proven to be outside DigiCert infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root.

CAs must log actions taken based on CAA records, and document issuance prevented by CAA for feedback to the CA/Browser Forum. Issuing CAs must specify the domain names authorizing issuance in their CPS.

The Issuer CA shall ensure that all communication between the Issuer CA and an RA regarding certificate issuance or changes in the status of a Certificate are made using secure and auditable methods. If databases or other sources are used to confirm sensitive or confidential attributes of an individual subscriber, then that sensitive information shall be protected and securely exchanged in a confidential and tamper-evident manner, protected from unauthorized access, and tracked using an auditable chain of custody.

For publicly-trusted TLS Certificates, Issuer CAs shall develop, maintain, and implement documented procedures

that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under the CABF Baseline Requirements.

4.2.2 Approval or Rejection of Certificate Applications

The Issuer CA shall reject any certificate application that cannot be verified. The Issuer CA shall not issue Certificates containing a new gTLD under consideration but not yet approved by ICANN. The Issuer CA or RA may also reject a certificate application on any reasonable basis, including if the Certificate could damage the Issuer CA's business or reputation. Issuer CAs shall not issue certificates containing internal names. Issuer CAs are not required to provide a reason for rejecting a certificate application.

Issuer CAs and RAs shall follow industry standards when approving and issuing Certificates. The Issuer CA or RA shall contractually require subscribers to verify the information in a Certificate prior to using the Certificate.

4.2.3 Time to Process Certificate Applications

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between the PKI participants. Identity shall be established no more than 30 days before initial issuance of Level 3 and 4 Certificates.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Issuer CAs shall verify the source of a certificate request before issuance. The Issuer CA and any RA shall protect databases under their control and that are used to confirm Subscriber identity information from unauthorized modification or use. The Issuer CA shall perform its actions during the certificate issuance process in a secure manner. Certificate issuance by the Root CA requires an individual authorized by the Issuer CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Issuer CA or RA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

The passage of time after delivery or notice of issuance of a Certificate to the Subscriber or the actual use of a Certificate constitutes the Subscriber's acceptance of the Certificate.

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate; or
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The Issuer CA shall publish all CA Certificates to the Issuer CA's repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The certificate shall be used lawfully in accordance with DigiCert's Subscriber Agreement the terms of this CP and the relevant CPS.

All Subscribers shall protect their Private Keys from unauthorized use or disclosure by third parties and shall use their Private Keys only for their intended purpose in accordance with section 9.6.3.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall use software that is compliant with X.509 and applicable IETF PKIX standards. The Issuer CA shall specify restrictions on the use of a Certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP).

Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties. A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. Relying on a digital signature or Certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

An Issuer CA may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the associated Private Key has not been compromised,
3. the Subscriber and attributes remain consistent, and
4. re-verification of subscriber identity is not required by Section 3.3.1.

An Issuer CA may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services. Issuer CAs may renew a certificate after expiration if the relevant industry permits such practices.

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew the expiring certificate to maintain continuity of Certificate usage.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates. An Issuer CA may perform renewal of its subscriber Certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

The Issuer CA may require reconfirmation or verification of the information in a Certificate prior to renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

The Issuer CA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The passage of time after delivery or notice of issuance of the Certificate to the Subscriber, or actual use of the Certificate, constitutes the Subscriber's acceptance of it.

4.6.6 Publication of the Renewal Certificate by the CA

The Issuer CA shall publish all renewed CA Certificates to the Issuer CA's repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.7 CERTIFICATE RE-KEY

Re-keying a Certificate consists of creating a new Certificate with a different Public Key (and serial number) while retaining the remaining contents and attributes of the subject in the old Certificate.

4.7.1 Circumstance for Certificate Rekey

Subscribers requesting re-key should identify and authenticate themselves as permitted by Section 3.3.1.

4.7.2 Who May Request Certification of a New Public Key

Only the subject of the Certificate, an authorized representative for an Organizational certificate, or the PKI sponsor may request re-key. The Issuer CA or an RA may initiate certificate re-key at the request of the certificate subject or at its own discretion.

4.7.3 Processing Certificate Rekey Requests

Re-key requests are only accepted from the subject of the Certificate, an authorized representative for an Organizational certificate, or the PKI sponsor. At a minimum, the Issuer CA shall comply with section 3.3.1 in identifying and authenticating the Subscriber or PKI sponsor prior to rekeying the Certificate.

4.7.4 Notification of Certificate Rekey to Subscriber

The Issuer CA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

The passage of time after delivery or notice of issuance of the Certificate to the Subscriber or the actual use of the Certificate constitutes the Subscriber's acceptance of it.

4.7.6 Publication of the Rekeyed Certificate by the CA

The Issuer CA shall publish rekeyed CA Certificates to the Issuer CA's repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstance for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CP. The new Certificate may have the same or a different subject Public Key.

4.8.2 Who May Request Certificate Modification

The Issuer CA may modify a Certificate at the request of the certificate subject or in its own discretion.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, the Issuer CA shall verify any information that will change in the modified Certificate. The Issuer CA may issue the modified Certificate only after completing the verification process on all modified information. The validity period of a modified Certificate must not extend beyond the applicable time limits found in section 3.3.1 or 6.3.2.

RAs shall perform identification and authentication of all modified Subscriber information in terms of Section 3.2

4.8.4 Notification of Certificate Modification to Subscriber

The Issuer CA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

The passage of time after delivery or notice of issuance of the Certificate to the Subscriber or actual use of the Certificate constitutes the Subscriber's acceptance of it.

4.8.6 Publication of the Modified Certificate by the CA

The Issuer CA shall publish modified CA Certificates to the Issuer CA's repository.

4.8.7 Notification of Certificate Modification by the CA to Other Entities

No stipulation.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, the Issuer CA shall verify that the revocation request was made by Subscribers, an RA, an Issuing CA, and other entities listed in section 4.9.2 of this CP and the associated CPS. Other parties may submit Certificate Problem Reports to DigiCert to report reasonable cause to revoke the Certificate. Issuer CAs must provide evidence of the revocation authorization to DigiCert upon request.

4.9.1 Circumstances for Revocation

The Issuer CA shall revoke a Certificate within 24 hours after receipt and confirming one or more of the following occurred:

1. The Subscriber requests in writing that the Issuer CA revoke the Certificate;
2. The Subscriber notifies the Issuer CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The Issuer CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or

4. The Issuer CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon.

The Issuer CA should revoke a certificate within 24 hours and must revoke a Certificate within 5 days after receipt and confirming that one or more of the following occurred:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;
2. The Issuer CA obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
3. The Subscriber or the cross-certified CA breached a material obligation under this CP, the CPS, or the relevant agreement;
4. The Issuer CA confirms of any circumstance indicating that use of a FQDN, IP address, or email 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. For code signing, the Application Software Supplier requests revocation and the Issuer Ca does not intend to pursue an alternative course of action;
6. For code signing, the certificate is being used for Suspect Code;
7. The Issuer CA confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
8. The Issuer CA confirms a material change in the information contained in the Certificate;
9. The Issuer CA confirms that the Certificate was not issued in accordance with the CA/B forum baseline requirements or relevant browser policy this CP or the CPS;
10. The Issuer CA determines or confirms that any of the information appearing in the Certificate is inaccurate;
11. The Issuer CA's right to issue Certificates under the CA/B forum baseline requirements expires or is revoked or terminated, unless the Issuer CA has made arrangements to continue maintaining the CRL/OCSP Repository;
12. Revocation is required by this CP and/or the CPS; or
13. The Issuer CA 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.

The Issuer CA should revoke a Certificate if the Issuer CA is aware that:

1. Either the Subscriber's or the Issuer CA's obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. The Issuer CA received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. The Issuer CA ceased operations and did not arrange for another CA to provide revocation support for the Certificate;
4. The technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others;
5. The Subscriber was added as a denied party or prohibited person to a blacklist, or is

- operating from a destination prohibited under U.S. law; or
6. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware or other harmful content, including any code that is downloaded onto a user's system without their consent.

The Issuer CA shall revoke a Certificate if the binding between the subject and the subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

The Issuer CA will revoke a Subordinate CA Certificate within seven (7) days after receiving and confirming one or more of the following occurred:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuer CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The Issuer CA 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. The Issuer CA obtains evidence that the CA Certificate was misused;
5. The Issuer CA confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with the CA/B forum baseline requirements or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuer CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. The Issuer CA or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. The Issuer CA's or the Subordinate CA's right to issue Certificates under the baseline requirements expires or is revoked or terminated, unless the Issuer CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuer 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.

If a Certificate expresses an organizational affiliation, the Issuer CA or the RA shall require the Affiliated Organization to inform it if the subscriber affiliation changes. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, then the Issuer CA shall revoke any Certificates issued to that Subscriber containing the organizational affiliation. If an Affiliated Organization terminates its relationship with the Issuer CA or RA such that it no longer provides affiliation information, the Issuer CA shall revoke all Certificates affiliated with that Affiliated Organization.

An Issuer CA or cross-certified entity shall request revocation of its DigiCert-issued cross-Certificate if it no longer meets the stipulations of DigiCert's policies, as indicated by DigiCert's policy OIDs in Certificates or those listed in the policy mapping extension of the cross-Certificate.

4.9.2 Who Can Request Revocation

The Issuer CA or RA shall accept revocation requests from authenticated and authorized parties, such as the certificate Subscriber or the Affiliated Organization named in a Certificate. The Issuer CA or RA may establish procedures that allow other entities to request Certificate revocation for fraud or misuse. The Issuer CA shall revoke a Certificate if it receives sufficient evidence of compromise or loss of the Private Key. The Issuer CA may revoke a Certificate of its own volition without reason, even if no other entity has requested revocation.

Regarding code signing certificates, Issuer CAs that issue code signing certificates must provide Anti- Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected Private Key

Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. Issuer CAs must publicly disclose the instructions on its website.

4.9.3 Procedure for Revocation Request

The Issuer CA shall provide a process for Subscribers to request revocation of their own Certificates. The process must be described in the Issuer CA's CPS.

The Issuer CA shall provide Subscribers, Relying Parties, application software suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The Issuer CA shall publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS. The Issuer CA shall maintain a continuous 24/7 ability to internally respond to any high priority Certificate problem reports. If appropriate, the Issuer CA or the RA may forward complaints to law enforcement.

The Issuer CA or RA shall authenticate and log each revocation request. The Issuer CA 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 or a problem report investigation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, the Issuer CA or RA shall investigate the alleged basis for the revocation request.

CA/RA Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CA's/RA's Subdomain. Issuer CAs shall authenticate the identity of Administrators before permitting them to perform revocation functions.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified. Issuer CAs and RAs are required to report the suspected compromise of their CA or RA Private Key and request revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

Subscribers shall request revocation as soon as possible if the Private Key corresponding to the Certificate is lost or compromised or if the certificate data is no longer valid. The Issuer CA may extend revocation grace periods on a case-by-case basis if it does not violate this CP, the CPS, or any of the relevant requirements as listed in the sources of section 1.6.3.

4.9.5 Time within which CA Must Process the Revocation Request

An Issuer CA shall revoke a Certificate within one hour of receiving appropriate instruction from the DCPA. An Issuer CA shall revoke the CA Certificate of a subordinate or cross-signed CA as soon as practical after receiving proper notice that the subordinate or cross-signed CA has been compromised. Except as otherwise set forth in section 4.9.1.2 of the Baseline Requirements, if an Issuer CA or the DCPA determines that immediate revocation is not practical, because the potential risks of revocation outweigh the risks caused by the compromise, then the Issuer CA and the DCPA shall jointly determine the appropriate process to follow in order to promptly revoke the subordinate or cross-signed CA Certificate.

Within 24 hours after receiving a Certificate problem report or a revocation request, the Issuer CA shall investigate the facts and circumstances involved and 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, the Issuer CA shall work 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 the CA 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 the Issuer CA should 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.

The Issuer CA shall revoke other Certificates as quickly as practical after validating the revocation request.

Issuer CAs and RAs that issue code signing certificates shall comply with the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly Trusted Code Signing Certificates in section 13.1.5.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on the information listed in a Certificate, a Relying Party shall confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7 CRL Issuance Frequency

4.9.8 Maximum Latency for CRLs

CRLs are posted to the DigiCert Repository within a commercially reasonable time after generation.

4.9.9 On-line Revocation/Status Checking Availability

The Issuer CA shall ensure that the certificate status information distributed by it on-line meets or exceeds the requirements for CRL issuance and latency stated in sections 4.9.5, 4.9.7 and 4.9.8.

OCSP responses must conform to RFC 6960 and/or RFC 5019. OCSP responses must either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960 and/or RFC 5019.

4.9.10 On-line Revocation Checking Requirements

A relying party shall confirm the validity of a Certificate via CRL or OCSP in accordance with section 4.9.6 prior to relying on the Certificate.

Issuer CAs shall support an OCSP capability using the GET method for Certificates issued in accordance with the Baseline Requirements.

Issuer CAs shall configure OCSP responses and validity periods in accordance with section 4.9.10 of the Baseline Requirements.

If the OCSP responder receives a request for status of a certificate serial number that is “unused”, then the responder shall not respond with a “good” status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5 of the Baseline Requirements, this CPS and the CP, the responder must not respond with a “good” status for such requests. “unused” if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

An Issuer CA may use other methods to publicize revoked Certificates, provided that:

1. the alternative method is described in its CPS,
2. the alternative method provides authentication and integrity services commensurate with the assurance level of the Certificate being verified, and
3. the alternative method meets the issuance and latency requirements for CRLs stated in sections 4.9.5, 4.9.7, and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

The Issuer CA or the RA shall use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that its Private Key has been compromised. The Issuer CA must have the ability to transition any revocation reason to code to “key compromise”. If a Certificate is revoked because of compromise or suspected compromise, the Issuer CA shall issue a CRL within 18 hours after it receives notice of the compromise or suspected compromise.

4.9.13 Circumstances for Suspension

Not applicable.

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

Issuer CAs shall make the status of public certificates is available via either CRL and/or an OCSP responder. For publicly-trusted TLS certificates, revocation entries on a CRL or OCSP Response shall not be removed until after the expiration of the revoked Certificate. Issuer CAs shall make certificate If using a CRL, the Issuer CA shall list revoked Certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the Certificate's validity period, except for Code Signing Certificates and EV Code Signing Certificates, which shall remain on the CRL for at least 10 years following the Certificate's validity period.

4.10.2 Service Availability

Issuer CAs for publicly-trusted TLS shall provide certificate status services 24x7. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by the Issuer CA.

The Issuer CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The Issuer CA shall maintain a 24x7 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.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

The Issuer CA shall allow Subscribers to end their subscription to certificate services by having their Certificate revoked or by allowing the Certificate or applicable Subscriber Agreement to expire without renewal.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy Practices

Issuer CAs shall not escrow CA Private Keys. Issuer CAs may escrow Subscriber key management keys to provide key recovery services. Issuer CAs shall encrypt and protect escrowed Private Keys with at least the level of security used to generate and deliver the Private Key. Enterprise customers utilizing key escrow software provided by DigiCert may escrow keys within their infrastructure.

Subscribers and other authorized entities may request recovery of an escrowed (decryption) Private Key. Entities escrowing Private Keys shall have personnel controls in place that prevent unauthorized access to Private Keys. Key recovery requests can only be made for one of the following reasons:

1. The Subscriber has lost or damaged the private-key token,
2. The Subscriber is not available or is no longer part of the organization that contracted with the Issuer CA for Private Key escrow,
3. The Private Key is part of a required investigation or audit,
4. The requester has authorization from a competent legal authority to access the communication that is encrypted using the key,
5. If key recovery is required by law or governmental regulation, or
6. If the entity contracting with the Issuer CA for escrow of the Private Key indicates that key

recovery is mission critical or mission essential.

An entity receiving Private Key escrow services shall:

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 escrowed keys only for properly authenticated and authorized requests for recovery, and
5. 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

Issuer CAs that support session key encapsulation and recovery shall describe their practices in their CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The Issuer CA shall perform its CA operations from a secure data center equipped with logical and physical controls that make the CA operations inaccessible to non-trusted personnel. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records. RAs must protect their equipment from unauthorized access in a manner that is appropriate to the level of threat to the RA, including protecting equipment from unauthorized access while the cryptographic module is installed and activated and implementing physical access controls to reduce the risk of equipment tampering, even when the cryptographic module is not installed and activated.

5.1.2 Physical Access

Each Issuer CA and each RA shall protect its equipment (including certificate status servers) from unauthorized access and shall implement physical controls to reduce the risk of equipment tampering. The Issuer CA and all RAs shall store all removable media and paper containing sensitive plain-text information related to CA or RA operations in secure containers. The security mechanisms should be commensurate with the level of threat to the equipment and data.

The Issuer CA shall manually or electronically monitor its systems for unauthorized access at all times, maintain an access log that is inspected periodically, and require two-person physical access to the CA hardware and systems. An Issuer CA shall deactivate and securely store its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA equipment or Private Keys.

If the facility housing the CA equipment is ever left unattended, the Issuer CA's administrators shall verify that:

1. the CA is in a state appropriate to the current mode of operation,
2. the security containers are properly secured
3. physical security systems (e.g., door locks, vent covers) are functioning properly, and
4. the area is secured against unauthorized access.

The Issuer CA shall make a person or group of persons explicitly responsible for making security checks. If a group of persons is responsible, the Issuer CA shall maintain a log that identifies who performed the security check. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and Air Conditioning

The Issuer CA and RAs shall maintain a backup power supply and sufficient environmental controls to protect the CA systems and allow the CA to automatically finish pending operations and record the state of equipment before a lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

The Issuer CA and RAs shall protect its CA equipment from water exposure.

5.1.5 Fire Prevention and Protection

The Issuer CA and RAs shall use facilities equipped with fire suppression mechanisms.

5.1.6 Media Storage

Issuer CAs and RAs shall protect all media from accidental damage, environmental hazards, and unauthorized physical access. Each Issuer CA and each RA shall duplicate and store its audit and archive information in a backup location that is separate from its primary operations facility.

5.1.7 Waste Disposal

Paper waste containing sensitive data shall be shredded before disposal. Sensitive data on magnetic or other digital media must be permanently erased before disposal

5.1.8 Off-site Backup

The Issuer CA or RA shall make weekly system backups sufficient to recover from system failure and shall store the backups, including at least one full backup copy, at an offsite location that has procedural and physical controls that are commensurate with its operational location.

5.1.9 Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under this Section 5.1 apply equally to any Certificate Status Hosting, CMS or external RA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

CA and RA personnel acting in trusted roles include CA and RA system administration personnel and personnel involved with identity vetting and the issuance and revocation of Certificates. Issuer CAs and RAs shall distribute the functions and duties performed by persons in trusted roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. Senior management of the Issuer CA or the RA shall be responsible for appointing individuals to trusted roles. A list of such personnel shall be maintained and reviewed annually.

The following five trusted roles are defined by this CP, although an Issuer CA or RA may define additional ones:

5.2.1.1 CA Administrators

The CA Administrator is responsible for the installation and configuration of the CA software, including key generation, user and CA accounts, audit parameters, key backup, and key management. The CA Administrator is responsible for performing and securely storing regular system backups of the CA system. Administrators may not issue certificates to Subscribers.

5.2.1.2 Registration Officers – CMS, RA, Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates.

5.2.1.3 System Administrator/ System Engineer (Operator)

The System Administrator, System Engineer, or CA Operator is responsible for installing and configuring critical CA system hardware. The System Administrator / Engineer is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4 Internal Auditor Role

The Internal Auditor Role is responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if the Issuer CA or RA is operating in accordance with this CP.

5.2.1.5 RA Administrators

RA Administrators install, configure and manage the RA software.

5.2.2 Number of Persons Required per Task

Policy and control procedures must be in place to ensure segregation of duties based on job responsibilities. Each Issuer CA shall require that at least two people acting in a trusted role take action for the most sensitive tasks, such as activating the Issuer CA's Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system, but logical access shall not be achieved using personnel that serve in the Internal Auditor role. Physical access to the CAs does not constitute a task as defined in this section.

5.2.3 Identification and Authentication for each Role

Issuer CA personnel shall authenticate themselves to the certificate management system before they are allowed access to the systems necessary to perform their trusted roles.

5.2.4 Roles Requiring Separation of Duties

Individual personnel shall be specifically designated to the five roles defined in Section 5.2.1 above. Individuals designated as Registration Officer or Administrator may also assume the Operator role. An Internal Auditor may not assume any other role.

The Issuer CA and RA may enforce separation of duties using CA equipment, procedurally, or by both means. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume multiple identities at the same time.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for the operation of the DigiCert PKI and compliance with this CP. Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, Issuer CAs shall verify the identity and trustworthiness of such person.

Managerial personnel involved in time-stamping operations must possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures.

The Issuer CA or the RA shall assess that individuals assigned to trusted roles perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background Check Procedures

The Issuer CA and RA shall require each person fulfilling a trusted role to undergo identity verification, background checks, and adjudication prior to acting in the role. Background checks shall be repeated for personnel holding Trusted Positions at least every five (5) years.

These checks include verification of the individual's identity, employment history, education, character references, social security number, previous residences, driving records, professional references, and criminal background. These procedures shall be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The Issuer CA or RA shall require each individual to appear in-person before a trusted agent whose responsibility it is to verify identity. The trusted agent shall verify the identity of the individual using at least one form of government-issued photo identification. Checks of

previous residences are over the past three years. All other checks are for the prior five years. The Issuer CA or RA shall verify the highest education degree obtained regardless of the date awarded and shall refresh all background checks at least every five years. Based upon the information obtained, a competent adjudication authority within the Issuer CA or RA shall adjudicate whether the individual is suitable for the position to which they will be assigned.

5.3.3 Training Requirements

The Issuer CA shall provide skills training in the Issuer CA's PKI operations for the personnel performing information verification duties including:

1. basic Public Key Infrastructure (PKI) knowledge;
2. software versions used by the Issuer CA;
3. authentication and verification policies and procedures;
4. CA/RA security principles 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. CA/Browser Forum Guidelines and other applicable industry and government guidelines.

Issuer CAs shall maintain a record of who received training. Issuer CAs and RAs shall ensure that Registration Officers have the minimum skills necessary to satisfactorily perform validation duties before they are granted validation privileges.. Issuer CAs shall require all Registration Officers performing information verification duties to pass an examination provided by the Issuer CA on the information verification requirements outlined in the Baseline Requirements and other CABF documents.

Issuer CAs and RAs involved with the operation of CMS shall ensure that all personnel who perform duties involving the CMS receive comprehensive training. Issuer CAs and RAs shall create a training (awareness) plan to address any significant change to CMS operations and shall document the execution of the plan.

5.3.4 Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. The Issuer CA or RA shall make individuals acting in relevant trusted roles aware of any changes to the Issuer CA's or RA's operations as necessary for them to perform their role. If such operations change, the Issuer CA or RA shall provide documented training, in accordance with an executed training plan, to all trusted roles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Issuer CA or RA employees and agents failing to comply with this CP, whether through negligence or malicious intent, shall be subject to policies and procedures maintained by the Issuer CA or RA to describe administrative or disciplinary actions, up to and including termination of employment or agency and criminal sanctions.

5.3.7 Independent Contractor Requirements

Any Issuer CA or RA allowing independent contractors to be assigned to perform trusted roles shall require that they agree to the obligations under this Section 5 (Facility, Management, and Operational Controls), meet the requirements of section 5.3.1, 5.3.2, and are held to the sanctions stated above in Section 5.3.6 by the Issuer CA.

5.3.8 Documentation Supplied to Personnel

Issuer CAs and RAs shall provide personnel in trusted roles with the documentation necessary to perform their duties.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

Issuer CA and RA systems (including any CMS) shall require identification and authentication at system logon. Important system actions shall be logged to establish the accountability of the operators who initiate such actions.

Issuer CAs and RAs shall enable all essential event auditing capabilities of its CA or RA applications in order to record all events related to the security of the CA or RA, including those listed below. A message from any source received by the Issuer CA requesting an action related to the operational state of the CA is an auditable event. If the Issuer CA's applications cannot automatically record an event, the Issuer CA shall implement manual procedures to satisfy the requirements. For each event, the Issuer CA shall record the relevant:

1. date and time;
2. type of event;
success or failure; and
3. user or system that caused the event or initiated the action.

The Issuer CA shall make all event records available to its auditors as proof of the Issuer CA's practices. Logs shall be maintained to the standard per the requirements of the relevant policies and programs.

Issuer CAs shall record at least the following events:

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, renewal, and re-key requests, and revocation;
 - b. All verification activities stipulated in the CABF Requirements and the Issuer CA CPS;
 - 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 MUST include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of Processing Log

The Issuer CA or RA shall make system and file integrity checks, and make a vulnerability assessment as required by industry standards. The Issuer CA or RA may use automated tools to scan for anomalies or specific conditions. During its review, the Issuer CA or RA shall verify that the logs

have not been tampered with, examine any statistically significant set of security audit data generated since the last review, and make a reasonable search for any evidence of malicious activity. The Issuer CA or RA shall briefly inspect all log entries and investigate any detected anomalies or irregularities. The Issuer CA or RA shall make a summary of the review available to its auditors upon request. The Issuer CA or RA shall document any actions taken as a result of a review.

5.4.3 Retention Period for Audit Log

The Issuer CA and RA shall retain audit logs on-site until after they are reviewed. Audit logs related to publicly trusted SSL/TLS certificates shall be retained for at least seven (7) years or in accordance with section 5.5.2. Issuer CAs shall make these audit logs available to auditors, as defined in section 8, available upon request.

5.4.4 Protection of Audit Log

The Issuer CA and RA shall implement procedures that protect archived data from destruction prior to the end of the audit log retention period. The Issuer CA and RA shall configure its systems and establish operational procedures to ensure that:

1. only authorized people have read access to logs;
2. only authorized people may archive audit logs; and
3. audit logs are not modified or deleted.

The Issuer CA and RA shall make records available if required for the purpose of providing evidence of the correct operation of time-stamping services for the purpose of legal proceedings. The Issuer CA shall make its audit logs available to auditors upon request.

5.4.5 Audit Log Backup Procedures

As required, the Issuer CA and RA shall make backups of audit logs and audit log summaries and save a copy of the audit log to a secure, off-site location.

5.4.6 Audit Collection System (internal vs. external)

The Issuer CA or RA may use automatic audit processes, provided that they are invoked at system startup and end only at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the DCPA shall be notified and determine whether to suspend the Issuer CA's or RA's operations until the problem is remedied.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The Issuer CA shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. The Issuer CA shall also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Issuer CA has in place to control such risks. The Issuer CA's auditors should review the security audit data checks for continuity and alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.7. RECORDS ARCHIVAL

The Issuer CA shall comply with any record retention policies that apply by law and retrieved as necessary by request of authorized parties. The Issuer CA shall include sufficient detail in archived records to show that a Certificate was issued in accordance with the CPS.

5.5.1 Types of Records Archived

The Issuer CA shall retain the following information in its archives (as such information pertains to

the Issuer CA's CA operations):

1. Any accreditation of the Issuer CA,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Certificate issuance, rekey, renewal, and revocation requests,
6. Rejection or acceptance of a certificate request,
7. Identity authentication data,
8. Any documentation related to the receipt or acceptance of a Certificate or token,
9. Subscriber Agreements,
10. Issued certificates,
11. A record of certificate re-keys,
12. Any data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Any changes to the Issuer CA's audit parameters,
15. Any attempt to delete or modify audit logs,
16. CA Key generation and destruction,
17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a revocation request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP or CPS.

5.5.2 Retention Period for Archive

For all other Certificates, the Issuer CA shall retain archived data for at least 7.5 years or according to their respective requirements and as contractually agreed upon.

5.5.3 Protection of Archive

The Issuer CA shall store its archived records at a secure off-site location in a manner that prevents unauthorized modification, substitution, or destruction. No unauthorized user may access, write, or delete the archives. If the original media cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media. The Issuer CA shall ensure that all archived information can be obtained within a reasonable timeframe through specified recovery services.

5.5.4 Archive Backup Procedures

If an Issuer CA or RA chooses to back up its archive records, then the Issuer CA or RA shall describe how its records are backed up and managed in its CPS or a referenced document.

5.5.5 Requirements for Time-stamping of Records

The Issuer CA shall automatically time-stamp archive records as they are created. Cryptographic time-stamping of archive records is not required; however, the Issuer CA shall synchronize its system time at least every eight hours using a real time value traceable to a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6 Archive Collection System (internal or external)

The Issuer CA shall collect archive information internally.

5.5.7 Procedures to Obtain and Verify Archive Information

The Issuer CA may archive data manually or automatically. If automatic archival is implemented, the Issuer CA shall synchronize its archived data on a daily basis.

The Issuer CA may allow Subscribers to obtain a copy of their archived information. Otherwise, the Issuer CA shall restrict access to archive data to authorized personnel in accordance with the Issuer CA's internal security policy and shall not release any archived information except as allowed by law. CAs shall state in their CPS the practices of how they create, verify, package, transmit, and store archived information.

5.6 KEY CHANGEOVER

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The Issuer CA shall develop and implement procedures to be followed in the event of a serious security incident or system compromise. Required documentation includes, but is not limited to, an Incident Response Plan, a Disaster Recovery, or Business Continuity Plan (DR/BCP), and related resources. The Issuer CA shall review, test, and update its Incident Response Plan and DR/BCP, and supporting procedures, at least annually. Issuer CAs for publicly-trusted TLS shall document in these procedures how it will notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

The Issuer CA shall require that any CMS have documented incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, the Issuer CA shall revoke all Certificates issued to the CMS, if applicable. The Issuer CA and its RAs shall also assess any damage caused by the CMS compromise, revoke all potentially compromised Subscriber Certificates, notify affected subscribers of the revocation, and re-establish the operation of the CMS.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The Issuer CA shall make regular back-up copies of its Private Keys and store them in a secure separate location. The Issuer CA shall also make regular system back-ups on at least a weekly basis. If a disaster causes the Issuer CA's operations to become inoperative, the Issuer CA shall, after ensuring the integrity of the CA systems, re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. The Issuer CA shall give priority to reestablishing the generation of certificate status information. If the Private Keys are destroyed, the Issuer CA shall reestablish operations as quickly as possible, giving priority to generating new Key Pairs.

5.7.3 Entity Private Key Compromise Procedures

If the Issuer CA suspects that a CA Private Key is compromised or lost then the Issuer CA shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action in accordance with internal and external requirements as listed in section 1.1. Issuer CA personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures should be taken to prevent a reoccurrence.

Following revocation of a CA Certificate and implementation of the Issuer CA's Incident Response Plan, the Issuer CA shall generate a new CA Key Pair and sign a new CA Certificate in accordance with its CPS. The Issuer CA shall distribute the new self-signed Certificate in accordance with Section 6.1.4.

5.7.4 Business Continuity Capabilities after a Disaster

Stated goals of the Issuer CA's DR/BCP shall include that certificate status services be minimally affected by any disaster involving the Issuer CA's primary facility and that other services resume as quickly as possible following a disaster. The Issuer CA shall establish a secure facility in at least one secondary, geographically diverse location to ensure that its directory and on-line status servers, if any, remain operational in the event of a physical disaster at the Issuer CA's main site. The Issuer CA shall provide notice at the earliest feasible time to all interested parties if a disaster physically damages the Issuer CA's equipment or destroys all copies of the Issuer CA's signature keys.

5.8 CA OR RA TERMINATION

If an Issuer CA's operations are terminated, the Issuer CA shall provide notice to interested parties and shall transfer its responsibilities and records to successor entities. The Issuer CA may allow a successor to re-issue Certificates if the successor has all relevant permissions to do so and has operations that are at least as secure as the Issuer CA's. If a qualified successor does not exist, the Issuer CA shall transfer all relevant records to a government supervisory or legal body.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

Issuer CAs shall generate cryptographic keying material on a FIPS 140-2 level 3 validated cryptographic module using multiple individuals acting in trusted roles. When generating key material, the Issuer CA shall create auditable evidence to show that the Issuer CA enforced role separation and followed its key generation process.

An independent third party shall validate that each CA key each Root CA Key is generated in accordance with this CP either by having the independent third party witness the key generation or by examining a signed and documented record of the key generation.

Subscribers who generate their own keys shall use a FIPS-approved method and either a validated hardware or validated software cryptographic module, depending on the level of assurance desired. Issuer CAs shall not generate key pairs for publicly trusted end-entity TLS Certificates and will not accept a certificate request using a Key Pair previously generated by the Issuer CA. Keys for Level 3 Hardware or Level 4 Biometric Certificates must be generated on validated hardware cryptographic modules using a FIPS-approved method. For publicly-trusted TLS Certificates, Issuer CAs shall reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 of CA/Browser Baseline Requirements or if it has a known weak Private Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>). The Issuer CA must reject the Subscriber Certificate request if it has an extendedKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280].

6.1.2 Private Key Delivery to Subscriber

If the Issuer CA, a CMS, or an RA generates keys on behalf of the Subscriber, then the entity generating the key shall deliver the Private Key securely (encrypted) to the Subscriber. The entity may deliver Private Keys to Subscribers electronically or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are provided, the key generator may not retain a copy of the Subscriber's Private Key after delivery;
2. The key generator shall protect the Private Key from activation, compromise, or modification during the delivery process;
3. The Subscriber shall acknowledge receipt of the Private Key(s); and
4. The key generator shall deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
 - a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
 - b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

SSL/TLS and S/MIME email signature certificates shall not be distributed as PKCS#12 packages. S/MIME encryption certificates can be distributed as PKCS#12 packages using secure channels and sufficiently secure passwords sent out of band from the package.

6.1.3 Public Key Delivery to Certificate Issuer

Subscribers should deliver their Public Keys to the Issuer CA in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key.

6.1.4 CA Public Key Delivery to Relying Parties

The Issuer CA shall provide its Public Keys to Relying Parties in a secure fashion and in a manner that precludes substitution attacks. The Issuer CA may deliver its CA Public Keys to Relying Parties as:

- specified in a certificate validation or path discovery policy file;
- trust anchors in commercial browsers and operating system root stores; and/or
- roots signed by other CAs.

The Issuer CA may distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. All accreditation authorities supporting DigiCert Certificates and all application software providers are permitted to redistribute any Root Certificate that is issued under this CP.

6.1.5 Key Sizes

For signing Certificates issued within the policy OID arcs of 2.16.840.1.114412.1, 2.16.840.1.114412.2, or 2.16.840.1.114412.4, the legacy arcs referenced in section 1.1, and for signing CRLs and certificate status server responses for such Certificates, the Issuer CAs shall use:

- 2048-bit or greater RSA Key (with a modulus size in bits divisible by 8);
- 256-bit ECDSA Key or greater with the matching Secure Hash Algorithm as required and a valid point on the elliptic curve; or
- a hash algorithm that is equally or more resistant to a collision attack allowed by the Mozilla Root Store policy and other references in sections 1.1 and 1.6.3.

The Issuer CA shall only issue end-entity Certificates that contain at least 2048-bit Public Keys for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms. The Issuer CA may require higher bit keys in its sole discretion if it is allowed by the programs and policies listed in section 1.1 and 1.6.3.

Any Root Certificates participating in the AATL program must be at least 3072-bit for RSA and 256-bit for ECDSA when issued on or after July 1, 2017.

The Issuer CA and Subscribers may fulfill the transmission security requirements of this CP using TLS or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys.

6.1.6 Public Key Parameters Generation and Quality Checking

The Issuer CA shall generate Public Key parameters for signature algorithms (the value of this public exponent shall be an odd number equal to three or more) and perform parameter quality checking in accordance with FIPS 186-2.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The Issuer CA shall include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Private Keys corresponding to Root CA Certificates must not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates; and
4. Certificates for OCSP Response verification

CA Certificates shall have two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the Certificate shall also set the digitalSignature bit.

The Issuer CA shall not issue Level 4 Certificates that are certified for both signing and encryption. The use of a single key for encryption and signature is discouraged, and Issuer CAs should issue Subscribers two Key Pairs—one for key management and one for digital signature and authentication. However, for support of legacy applications, other Certificates, including those at Levels 1, 2 and 3, may include a single key for use with encryption and signature. Such dual-use Certificates must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP,
2. never assert the non-repudiation key usage bit, and
3. not be used for authenticating data that will be verified on the basis of the dual-use Certificate at a future time.

Subscriber Certificates must assert key usages based on the intended application of the Key Pair, and cannot include anyExtendedKeyUsage

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The Issuer CA and all systems that sign OCSP responses or CRLs in order to provide certificate status services shall use cryptographic hardware modules validated to FIPS 140-2 Level 3.

Cryptographic module requirements for subscribers and registration authorities are shown in the table below.

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
Adobe Signing Certificates	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
Level 1 - Rudimentary	N/A	FIPS 140-2 Level 1 (Hardware or Software)
Level 2 – Basic	FIPS 140-2 Level 1 (Hardware or Software)	FIPS 140-2 Level 1 (Hardware or Software)

Level 3 - Medium	FIPS 140-2 Level 1 (Software) FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
Level 4, Medium Hardware, Biometric	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

For EV Code Signing Certificates, the Issuer CA shall ensure that the Private Key is properly generated, stored, and used in a cryptomodule that meets or exceeds the requirements of FIPS 140-2 level 2.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. Effective January 1, 2017, all cryptographic modules for Custodial Subscriber Key Stores for certificates issued at Levels 2, 3-US, 3-CBP, 4-US, and 4-CBP shall be no less than FIPS 140-2 Level 2 Hardware and authentication to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

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

The Issuer CA shall ensure that multiple trusted personnel are required to act in order to access and use an Issuer CA's Private Keys, including any Private Key backups.

6.2.3 Private Key Escrow

The Issuer CA shall not escrow its signature keys. Subscribers may not escrow their private signature keys. The Issuer CA may escrow Subscriber Private Keys used for encryption in order to provide key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

The Issuer CA shall backup its CA, CRL, and certificate status Private Keys under multi-person control and shall store at least one backup at a secure location. The Issuer CA shall protect all copies of its CA, CRL, and certificate status Private Keys in the same manner as the originals.

The Issuer CA may provide backup services for Private Keys that are not required to be maintained in cryptographic hardware. Access to Private Key backups shall be secured in a manner that only the Subscriber can control the Private Key. The Issuer CA may not backup Level 4 subscriber private signature keys. The Issuer CA may not store backup keys in a plain text form outside of the cryptographic module. Storage that contains backup keys shall provide security controls that are consistent with the protection provided by the Subscriber's cryptographic module.

6.2.5 Private Key Archival

The Issuer CA shall not archive its Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. The Issuer CA and RA shall never allow their Private Keys to exist in plain text outside of the cryptographic module. The Issuer CA shall only export its Private Keys from the cryptographic module to perform CA key backup procedures. When

transported between cryptographic modules, the Issuer CA shall encrypt the Private Key and protect the keys used for encryption from disclosure.

If the Issuer CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinated CA, then the Issuer CA will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

Issuer CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, shall securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

The Issuer CA shall store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3. Issuer CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

The Issuer CA shall activate its Private Keys in accordance with the specifications of the cryptographic module manufacturer.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. At a minimum, Subscribers must authenticate themselves to the cryptographic module before activating their Private Keys. Entry of activation data shall be protected from disclosure. Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. When deactivated, private keys shall be kept in encrypted form only and secured.

6.2.9 Method of Deactivating Private Key

The Issuer CA shall deactivate its Private Keys and store its cryptographic modules in secure containers when not in use. The Issuer CA shall prevent unauthorized access to any activated cryptographic modules.

6.2.10 Method of Destroying Private Key

The Issuer CA shall use individuals in trusted roles to destroy CA, RA, and status server Private Keys when they are 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. For software cryptographic modules, the Issuer CA may destroy the Private Keys by overwriting the data. For hardware cryptographic modules, the Issuer CA may destroy the Private Keys by executing a "zeroize" command. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The Issuer CA shall archive a copy of each Public Key.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All Certificates, including renewed Certificates, have maximum validity periods of:

Type	Private Key Use ¹⁰	Certificate Term
Publicly Trusted Root CAs	No stipulation	25 years
Root CAs Not Otherwise Restricted	No stipulation	100 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
IGTF Cross-certified Sub CA ¹¹	6 years	15 years
CRL and OCSP responder signing for DirecTrust	3 years	31 days
CRL and OCSP responder signing	3 years	No Stipulation ¹²
DV SSL/TLS	No stipulation	398 days
OV SSL/TLS	No stipulation	398 days
EV SSL/TLS	No stipulation	398 days
Code Signing Certificate issued to Subscriber under the Minimum Requirements for Code Signing Certificates or the EV Code Signing Guidelines	No stipulation	39 months
EV Code Signing Certificate issued to Signing Authority	No stipulation	123 months
Time Stamping Authority	15 months	135 months
Object Signing Certificate and Document Signing	No stipulation ^{13‡}	123 months
IGTF Client used for signatures	36 months	36 months
IGTF Client used for key management	36 months	36 months
Client for all other purposes (IGTF compliant)	36 months	36 months
Client for all other purposes (non IGTF certs)	No stipulation	60 months
IGTF on hardware	60 months	13 months

Participants shall cease all use of their key pairs after their usage periods have expired.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day.

Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

The Issuer CA may retire its CA Private Keys before the periods listed above to accommodate key changeover processes. The Issuer CA shall not issue a Subscriber Certificate with an expiration date that exceeds the Issuer CA's public key term stated in the table above or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

¹⁰ CA Private Keys may continue to be used to sign CRLs and OCSP responses.

¹¹ IGTF signing Certificates must have a lifetime that is at least twice the maximum lifetime of an end entity Certificate.

¹² Restrictions will be based on program requirements as listed in section 1.1 of this CPS.

The Issuer CA shall generate activation data that has sufficient strength to protect its Private Keys to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use. If the Issuer CA uses passwords as activation data for a signing key, the Issuer CA shall change the activation data upon rekey of the CA Certificate. The Issuer CA may 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.

When passwords are required, Subscribers shall generate passwords that meet the requirements specified by the CAB Forums Network Security Requirements.

6.4.2 Activation Data Protection

The Issuer CA shall protect data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- Memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The Issuer CA shall require personnel to memorize and not write down their password or share their passwords with other individuals. The Issuer CA shall implement processes to temporarily lock access to secure CA processes if a certain number of failed log-in attempts occur as set forth in the applicable CPS.

End-user Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

Issuer CA and RA functions take place on trustworthy systems in accordance with the standards documented in this CP and as contractually obligated.

6.5.1 Specific Computer Security Technical Requirements

The Issuer CA shall configure its systems, to:

1. authenticate the identity of users before permitting access to the system or applications;
2. manage the privileges of users and limit users to their assigned roles;
3. generate and archive audit records for all transactions;
4. enforce domain integrity boundaries for security critical processes; and
5. support recovery from key or system failure.

The Issuer CA shall authenticate and protect all communications between a trusted role and its CA system.

RAs shall ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

RAs shall logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs shall use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters. Inactivity log out timeframes shall be set and enforced through internal information security policies and procedures to ensure security.

Direct access to the RA's database maintaining Subscriber information shall be limited to Trusted Persons in the RA's operations group having a valid business reason for such access

All Certificate Status Servers interoperating with cross-certified environments must:

1. authenticate the identity of users before permitting access to the system or applications;
2. manage privileges to limit users to their assigned roles;
3. enforce domain integrity boundaries for security critical processes; and
4. support recovery from key or system failure.

A CMS must have the following computer security functions:

1. authenticate the identity of users before permitting access to the system or applications;
2. manage privileges of users to limit users to their assigned roles;
3. generate and archive audit records for all transactions (see Section 5.4);
4. enforce domain integrity boundaries for security critical processes; and
5. support recovery from key or system failure.

Issuer CAs shall enforce multi-factor authentication on any account capable of directly causing Certificate issuance.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

In operating its CA, the Issuer CA shall use only:

1. Commercial off-the-shelf software that was designed and developed under a formal and documented development methodology,
2. Hardware and software developed specifically for the Issuer CA by verified personnel, using a structured development approach and a controlled development environment,
3. Open source software that meets security requirements through software verification & validation and structured development/life-cycle management,
4. Hardware and software purchased and shipped in a fashion that reduces the likelihood of tampering, and
5. For CA operations, hardware and software that is dedicated only to performing the CA functions.

The Issuer CA shall take proper care to prevent malicious software from being loaded onto the CA equipment. The Issuer CA shall scan all hardware and software for malicious code on first use and periodically thereafter. The Issuer CA shall purchase or develop updates in the same manner as original equipment, and shall use trusted trained personnel to install the software and equipment. The Issuer CA shall not install any software on its CA systems that are not part of the CA's operations.

The Issuer CA shall use a formal configuration management methodology for installation and ongoing maintenance of any CMS. Any modifications and upgrades to a CMS shall be documented and controlled. The Issuer CA shall implement a mechanism for detecting unauthorized modification to a CMS.

6.6.2 Security Management Controls

The Issuer CA shall establish formal mechanisms to document, control, monitor, and maintain the installation and configuration of its CA systems, including any modifications or upgrades. The Issuer CA's change control processes shall include procedures to detect unauthorized modification to the Issuer CA's systems and data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. When loading software onto a CA system, the Issuer CA shall verify that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Issuer CA and RA functions are performed using networks secured in accordance with the standards documented in this CP to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

The Issuer CA shall document and control the configurations of its systems, including any upgrades or modifications made. The Issuer CA shall implement a process for detecting unauthorized modifications to its hardware or software and for installing and maintaining its systems.

The Issuer CA and its RAs shall implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CA systems. The Issuer CA shall implement the same network security controls to protect a CMS as used to protect its other CA equipment.

6.8 TIME-STAMPING

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

Issuer CAs shall ensure that the accuracy of clocks used for time-stamping are within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Issuer CAs shall generate 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)

Issuer CAs shall issue X.509 version 3 Certificates.

7.1.2 Certificate Extensions

Issuer CAs shall use certificate extensions in accordance with applicable industry standards, including RFC 5280. Issuer CAs shall not issue Certificates with a critical private extension. IGTF Certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125. For Root CA, Subordinate CA, and Subscriber certificates used for publicly-trusted TLS, Issuer CAs must abide by section 7.1.2 of the Baseline Requirements and configure the Certificate extensions to those requirements.

Certificates must contain the ExtendedKeyUsage extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. Certificates may not contain the anyEKU value. Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: must contain an EKU extension; and must not include the anyExtendedKeyUsage KeyPurposeld; and, must not include both the id-kp-serverAuth and id-kp-emailProtection KeyPurposelds in the same certificate. Technically Constrained Subordinate CA Certificates shall include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeld shall not appear in the EKU extension of publicly trusted certificates.

For TLS or S/MIME, the subjectAltName extension is populated in accordance with RFC 5280. For all web server certificates, the SubjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public IP address). The SubjectAltName extension may contain additional authenticated domain names or public IP addresses. For internationalized domain names, the Common Name is represented as a puny-code value and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

7.1.3 Algorithm Object Identifiers

Issuer CAs shall sign Certificates using one of the following algorithms:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 10 }

ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512 ⁴	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

If an Issuer CA signs Certificates using RSA with PSS padding, the Issuer CA may use an RSA signature with PSS padding with the following algorithms and OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Issuer CAs and Subscribers may generate Key Pairs using the following:

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }
id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]

Issuer CAs shall not issue SSL Certificates with a Reserved IP Address or Internal Name.

Issuer CAs for publicly-trusted TLS shall configure all keys and hash algorithms as specified in the CAB forum requirements in section 7.

⁴ This algorithm shall not be used for Certificates with public trust from Mozilla.

7.1.4 Name Forms

Issuer CAs shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 5280. Issuer CAs shall include a unique serial number. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. For CABF Requirements, the Issuer CA shall restrict OU fields from containing Subscriber information that is not verified in accordance with Section 3. Issuer CAs shall meet the requirements in section 7.1.4 of the Baseline Requirements for Issuer DNs.

Subject attributes must not contain only metadata such as ‘’, ‘-’, and ‘ ’ (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.5 Name Constraints

Issuer CAs may include name constraints in the nameConstraints field when appropriate.

For publicly-trusted TLS certificates, Issuer CAs must meet the requirements of section 7.1.5 of the Baseline Requirements and as the following sections specify.

7.1.5.1 Name-Constrained serverAuth CAs

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then a technically constrained Subordinate CA Certificate shall include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

- a) For each dNSName in permittedSubtrees, the Issuer CA shall confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements section 3.2.2.4.
- b) For each iPAddress range in permittedSubtrees, the Issuer CA shall confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
- c) For each DirectoryName in permittedSubtrees the Issuer CA shall confirm the Applicant's and/or Subsidiary's Organizational name(s) and location(s) such that end entity certificates issued from the subordinate CA Certificate will comply with section 7.1.2.4 and 7.1.2.5 of the Baseline Requirements.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate shall specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate shall include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate shall also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate shall include at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate shall include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate shall include at least one dNSName in permittedSubtrees.

7.1.5.2 Name-Constrained emailProtection CAs

If the technically constrained Subordinate CA certificate includes the id-kp-emailProtection extended key usage, it shall include the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

7.1.6 Certificate Policy Object Identifier

When an Issuer CA issues a Certificate containing one of the policy identifiers set forth in Section 1.2, it asserts that the Certificate is managed in accordance with the policy that is identified herein.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Issuer CAs should include brief statements in the Policy Qualifier field of the Certificate Policy extension. Certificates may contain a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the applicable CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL PROFILE

For revoked issuing CAs, the CRLReason indicated cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, Issuer CAs must omit the reasonCode entry extension, when not technically not capable of issuance. If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate from RFC 5280, section 5.3.1.

7.2.1 Version number(s)

Issuer CAs shall issue version 2 CRLs that conform to RFC 5280.

7.2.2 CRL and CRL Entry Extensions

Issuer CAs shall issue version 2 CRLs with CRL extensions that conform to RFC 5280.

7.3 OCSP PROFILE

Issuer CAs shall operate an OCSP service in accordance with RFC 6960.

Effective 2020-09-30, for publicly-trusted TLS, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus shall be present and asserted.

Effective 2020-09-30, for publicly-trusted TLS, the CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2 of this CP.

7.3.1 Version Number(s)

Issuer CAs shall support version 1 OCSP requests and responses.

7.3.2 OCSP Extensions

No stipulation.

The singleExtensions of an OCSP response shall not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies in this CP are designed to meet or exceed the requirements of generally accepted and developing industry standards, including the applicable versions of the WebTrust Principles and Criteria as required by the programs and policies of section 1.1 as applicable to each Issuer CA. All Issuer CAs shall ensure that audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

On at least an annual basis, Issuer CAs and any other participants contractually requiring an audit shall retain an independent auditor for a period in time audit who shall assess the Issuer CA's and other party's compliance with this CP and its CPS. This audit must cover CMSs, Sub CAs, RAs, and each status server that is specified in a certificate issued by the Issuer CA. Any independent entity interoperating within the DigiCert PKI shall submit its practices statement and the results of its compliance audit to the DCPA on an annual basis for review and approval.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The Issuer CA shall use an auditor that meets Section 8.2 of the CA/Browser Baseline Requirements.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Issuer CA shall utilize independent auditors that do not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the Issuer CA. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services.

8.4 TOPICS COVERED BY ASSESSMENT

The audit must conform to industry standards, cover the Issuer CA's compliance with its business practices disclosure, and evaluate the integrity of the Issuer CA's PKI operations. The audit must verify that each Issuer CA is compliant with this CP and any MOA between it and any other PKI.

Issuer CAs for publicly-trusted certificates shall undergo an audit in accordance with one of the following schemes:

1. "WebTrust for CAs v2.1 or newer" AND "WebTrust for CAs SSL Baseline with Network Security v2.3 or newer"; or
2. ETSI EN 319 411-1 v1.2.2, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).

Whichever scheme is chosen, it shall incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme. The audit shall be conducted by a Qualified Auditor, as specified in Section 8.2.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CP, the CPS, or any other contractual obligations related to the Issuer CA's services, then the DCPA shall notify any affected cross-certifying entity and any relevant government accrediting body. The Issuer CA shall submit the plan to the DCPA for approval and to any third party that the Issuer CA is legally obligated to satisfy. The DCPA may require additional action if necessary, to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates. DigiCert shall be entitled to suspend and/or terminate services through revocation or other actions as deemed by the DCPA to address the non-compliant Issuer CA.

8.6 COMMUNICATION OF RESULTS

The results of each audit shall be reported to the DCPA for review and approval. The results shall also be communicated to any third party entities entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of applicable audits shall be sent to Adobe within three months of

the completion.

CAs shall make its annual Audit Report publicly available no later than three (3) months after the end of the audit period if required by the program. In the event of a delay greater than three months, the CA shall provide an explanatory letter signed by the Qualified Auditor.

8.7 SELF-AUDITS

The Issuer CA shall perform regular internal audits of its operations, personnel, and compliance with this CP using a randomly selected sample of Certificates issued since the last internal audit. The Issuer CA shall self-audit at least three percent of SSL/TLS Certificates and EV Code Signing Certificates on a quarterly basis. Audits of other certificate types will be at the discretion of the CA to gain reasonable assurance of compliance to applicable root program requirements.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1 Certificate Issuance or Renewal Fees

Issuer CAs may charge fees for certificate issuance and renewal.

9.1.2 Certificate Access Fees

Issuer CAs may charge fees for access to their databases of Certificates.

9.1.3 Revocation or Status Information Access Fees

Issuer CAs shall not charge a fee as a condition of making the CRLs required by this CP available in a repository or otherwise available to Relying Parties. They shall, however, be entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. Issuer CAs shall not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without the Issuer CA's prior express written consent.

9.1.4 Fees for Other Services

Issuer CAs shall not charge a fee for access to this CP or their respective CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Issuer CAs shall maintain Errors and Omissions / Professional Liability Insurance of at least \$1 million per occurrence from an insurance company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

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

Issuer CAs shall specify what constitutes confidential information in its CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Issuer CAs may treat any information not listed as confidential in the CPS as public information.

9.3.3 Responsibility to Protect Confidential Information

Issuer CAs shall contractually obligate employees, agents, and contractors to protect confidential information. Issuer CAs shall provide training to employees on how to handle confidential information.

9.4 *PRIVACY OF PERSONAL INFORMATION*

9.4.1 Privacy Plan

Issuer CAs shall create and follow a publicly posted privacy policy that specifies how the Issuer CA handles personal information.

9.4.2 Information Treated as Private

Issuer CAs shall treat all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. The Issuer CA shall protect private information in its possession using a reasonable degree of care and appropriate safeguards. The Issuer CA shall not distribute Certificates that contain the UUID in the subject alternative name extension via publicly accessible repositories (e.g., LDAP, HTTP).

9.4.3 Information Not Deemed Private

Subject to local laws, private information does not include Certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information

Issuer CAs are responsible for securely storing and protecting private information.

9.4.5 Notice and Consent to Use Private Information

Subscribers must consent to the global transfer and publication of any personal data contained in Certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Issuer CAs may disclose private information, without notice, when required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 *INTELLECTUAL PROPERTY RIGHTS*

9.5.1 Property Rights in Certificates and Revocation Information

Issuer CAs retain all intellectual property rights in and to the Certificates and revocation information that they issue. DigiCert, Affiliates, and customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. DigiCert, Affiliates, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CP

Issuer CAs acknowledge that DigiCert retains all intellectual property rights in and to this CP.

9.5.3 Property Rights in Names

Subscribers and Applicants retain all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate and distinguished name within any Certificate issued to such Subscriber or Applicant.

9.5.4 Property Rights in Keys and Key Material

Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the Issuer CAs and end-user Subscribers that are the respective subjects of the Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all intellectual property rights in and to these key pairs. Without limiting the generality of the foregoing, DigiCert's root Public Keys and the Root Certificates containing them, including all Public Keys and self-signed Certificates, are the property of DigiCert. DigiCert licenses software and hardware manufacturers to reproduce such Root Certificates to place copies in trustworthy hardware devices or software.

9.5.5 Violation of Property Rights

Issuer CAs shall not knowingly violate the intellectual property rights of any third party

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

Issuer CAs must represent to DigiCert, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP and their CPS.

Subscriber Agreements may include additional representations and warranties that do not contradict or supersede this CP.

9.6.2 RA Representations and Warranties

At a minimum, Issuer CAs shall require RAs operating on their behalf to represent that they have followed this CP and the relevant CPS when participating in the issuance and management of Certificates.

Subscriber Agreements may include additional representations and warranties

9.6.3 Subscriber Representations and Warranties

DigiCert requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of DigiCert and the Certificate Beneficiaries. For TLS, prior to the issuance of a Certificate, DigiCert will obtain, for the express benefit of DigiCert and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with DigiCert, or
2. The Applicant's acknowledgement of the Terms of Use.

Prior to being issued and receiving a Certificate, each Subscriber shall represent to DigiCert and the Issuer CA that the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information and communication to the Issuer CA and RA,
3. Confirm the accuracy of Certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify the Issuer CA if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with this CP and the relevant CPS and Subscriber Agreement, including only installing SSL/TLS Server Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and
7. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

Subscriber Agreements may include additional representations and warranties

9.6.4 Relying Party Representations and Warranties

Relying Parties must follow the procedures and make the representations required by the relevant CPS and in the applicable Relying Party Agreement prior to relying on or using a Certificate.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

Except as expressly stated otherwise herein, an applicable extended warranty protection plan or as limited by law, DigiCert disclaims all warranties and obligations related to this CP.

9.8 LIMITATIONS OF LIABILITY

Issuer CAs may limit their liability to any extent not otherwise prohibited by this CP, provided that the Issuer CA remains responsible for complying with this CP and the Issuer CA's CPS.

To the extent DigiCert has issued and managed the Certificate(s) at issue in compliance with this CP and its CPS, DigiCert shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit DigiCert's and the applicable Affiliates' liability outside the context of any extended warranty protection program. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 INDEMNITIES

9.9.1 Indemnification by an Issuer CA

To the extent permitted by applicable law, Issuer CAs are required to indemnify DigiCert for any violation of this CP.

Issuer CAs shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the Issuer CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the Issuer CA where such claim, damage, or loss was directly caused by such Application Software Supplier'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 Issuer CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

Issuer CAs shall include any indemnification requirements for Subscribers in their CPS and in their Subscriber Agreements.

To the extent permitted by applicable law, Subscribers are required to indemnify Issuer CAs or RAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,

- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's Private Key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the intellectual property rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3 Indemnification by Relying Parties

Issuer CAs shall include any indemnification requirements for Relying Parties in their CPS.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP and any amendments are effective when published to DigiCert's online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CP as amended from time to time, shall remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

DigiCert will communicate the conditions and effect of this CP's termination via the DigiCert Repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert accepts digitally signed or paper notices related to this CP that are addressed to the locations specified in Section 2.2 of this CP. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DigiCert. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

For CAs participating in the AATL program, the Issuer CAs shall notify Adobe a month in advance of any updates or changes with the potential to affect compliance with the AATL program, including:

1. Additions of Root CAs and Subordinate CAs
2. Additional CPs at the Root CA level
3. Changes in Certificate issuance procedures
4. Terminations or transition of ownership of Root CAs or Subordinate CAs.

All Issuer CAs whose certificates are included in Mozilla's root program must notify Mozilla if:

1. Ownership or control of the CA's certificate(s) changes;
2. An organization other than the CA obtains control of an unconstrained intermediate certificate (as defined in section 5.3.2 of the Mozilla Root Store policy) that directly or transitively chains to the Issuer CA's included certificate(s);
3. Ownership or control of the Issuer CA's operations changes; or
4. There is a material change in the Issuer CA's operations (e.g., when the cryptographic hardware related to a certificate in Mozilla's root store is consequently moved from one secure location to another).

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The DCPA determines what amendments should be made to this CP. Amendments are made by

posting an updated version of the CP to the online repository. Updates supersede any designated or conflicting provisions of the referenced version of the CP. Controls are in place to reasonably ensure that this CP is not amended and published without the prior authorization of the DCPA. The DCPA reviews this CP annually.

9.12.2 Notification Mechanism and Period

DigiCert will post notice on its website of any proposed significant revisions to this CP. Although DigiCert may include a final date for receipt of comments and the proposed effective date, DigiCert is not required to have a fixed notice-and-comment period. DigiCert and the DCPA reserve the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The DCPA's decision to designate amendments as material or non-material shall be within the DCPA's sole discretion.

9.12.3 Circumstances under which OID Must Be Changed

If the DCPA determines an amendment necessitates a change in an OID, then the revised version of this CP will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13 DISPUTE RESOLUTION PROVISIONS

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Unless otherwise approved by DigiCert, the procedure to resolve disputes involving DigiCert require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Salt Lake County, Utah, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration

Before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution, a party must notify DigiCert of the dispute with a view to seek dispute resolution.

9.14 GOVERNING LAW

For disputes involving Qualified Certificates, the national law of the relevant Member State shall govern. For all other certificates, the laws of the state of Utah shall govern the interpretation, construction, and enforcement of this CP and all proceedings related hereunder, including tort claims, without regard to any conflicts of law principles, and Salt Lake County, Utah shall be the non-exclusive venue and shall have jurisdiction over such proceedings.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is subject to all applicable laws and regulations. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, each Issuer CA shall (i) be licensed in each jurisdiction where it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates, and (ii) meet the requirements of European data protection laws and shall establish and maintain appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

Issuer CAs shall contractually obligate each RA involved in Certificate issuance to comply with this CP and applicable industry guidelines. Issuer CAs shall contractually obligate parties using products and services issued under this CP, such as Subscribers and Relying Parties, to the relevant provisions herein. This CP does not give any third party rights under such agreements.

9.16.2 Assignment

Entities operating under this CP may not assign their rights or obligations without the prior written consent of DigiCert.

9.16.3 Severability

If a provision of this CP is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP will remain valid and enforceable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

DigiCert is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond DigiCert's reasonable control. The operation of the Internet is beyond DigiCert's reasonable control.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting DigiCert.

9.17 OTHER PROVISIONS

No stipulation.