CrossCert

Certification Practices Statement

Version 5.0

CrossCert, Inc.
7F, Halim building, Seocho Daero 320(1674-4, SeochoDong)
Seocho-gu, Seoul, 06633 Korea

Tel : +82-2-3019-5500
www.crosscert.com

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the CrossCert Certification Practices Statement (CPS) that outlines the principles and practices related to CrossCert's certification service. This CPS applies to all entities participating in or using CrossCert's certificate service, excluding participants in CrossCert's Private PKI services, which are not cross-certified or publicly trusted.

This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

Name of Policy/Guideline/Requirement Standard	**Location of Source Document/Language**
DigiCert Certificate Policy version 5.0	https://www.digicert.com/legal-repository/
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 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

If any inconsistency exists between this CPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this CPS.

This CPS is only one of several documents that control CrossCert's certification service. Other important documents include both private and public documents, such as the DigiCert's CP, CrossCert's agreements with its customers, Relying Party agreements, and CrossCert's privacy policy. CrossCert may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

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

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the CrossCert Certification Practices Statement and was approved for publication by the DigiCert Policy Authority (DCPA).

This document is the CrossCert Certification Practices Statement (CPS). Certificates contain object identifier values corresponding to the applicable Class of Certificate as listed in section 1.2 of the DigiCert's CP.

CrossCert issues Certificates containing the following OIDs / OID arcs:

Digitally Signed Object	Object Identifier (OID)
Level 1 Certificates – Personal	2.16.840.1.113733.1.7.23.1
Level 1 Certificates – Enterprise	2.16.840.1.113733.1.7.23.2
Level 2 Certificates	2.16.840.1.113733.1.7.23.3.2

All OIDs mentioned above belong to their respective owners. The specific OIDs used when objects are signed pursuant to this CPS are indicated in the object's respective Certificate Policies extension. For instance, when CrossCert issues a Certificate containing one of the above-specified policy identifiers for "Baseline Requirements," "Minimum Requirements," it asserts that the Certificate was issued and is managed in accordance with those applicable requirements and policies for the PKI participant.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

CrossCert operates certification authorities (CAs) that issue digital certificates. CrossCert performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs. General Information about CrossCert's products and services are available at www.crosscert.com.

In limited circumstances, root CAs owned by DigiCert are used to issue cross Certificates to external third parties operating their own PKIs. An external Issuer CA is an unaffiliated third party that is issued a subordinate CA Certificate by DigiCert where the Private Key associated with that CA Certificate is not maintained under the physical control of DigiCert.

All external subordinate CAs are prohibited, either technically or contractually, from issuing Certificates to domain names or IP addresses that a Subscriber does not legitimately own or control (i.e. issuance for purposes of "traffic management" is prohibited), and external subordinate CAs are required to implement procedures that are at least as restrictive as those found herein.

1.3.2. Registration Authorities and Other Delegated Third Parties

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). CrossCert and subordinate Issuer CAs may act as RAs for certificates they issue. Affiliates do not perform domain or IP address validation. Validation of domains for S/MIME Certificates cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

Except for the authentication of domain control or IP address verification performed solely by CrossCert in accordance with Section 3.2.2, CrossCert may delegate the performance of certain functions to third party Registration Authorities (RA) if it meets the requirements of the DigiCert CP and the relevant requirements listed in sections 1.1 and 1.6.3 of this CPS and the DigiCert CP. The specific role of an RA or Delegated Third Party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information.

CrossCert contractually obligates each Delegated Third Party to abide by the policies and industry standards that are applicable to that Delegated Third Party's delegated responsibilities.

1.3.3. Subscribers

Subscribers use CrossCert's services and PKI to support transactions and communications. Subscribers under this CPS 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, may refer to the Subject of the Certificate and the entity that contracted with CrossCert 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 CrossCert 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 CPS, 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 CrossCert. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate. A Relying party may, or may not also be a Subscriber of the CrossCert Public PKI hierarchy.

1.3.5. Other Participants

Other participants include Accreditation Authorities (such as Policy Management Authorities, Federation Operators, Application Software Vendors, and applicable Community-of-Interest sponsors); Bridge CAs and CAs cross-certified with DigiCert's CAs that serve as trust anchors in other PKI communities; and Time Source Entities, Time Stamp Token Requesters, and Time Stamp Verifiers involved in trusted time stamping. Accreditation Authorities are granted an unlimited right to re-distribute DigiCert's root Certificates and related information in connection with the accreditation.

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.

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 the DigiCert 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 CPS 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 the DigiCert CP, by any CPS (including this one) under which the certificate has been issued and any agreements with Subscribers.

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within 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 CPS.
This CPS covers several different types of end entity Certificates with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate	Appropriate Use
Level 1 Client Certificates - Enterprise and Class 1 and 2 Certificates	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 2 Client Certificates	Issued to identity-vetted individuals. Certificates specify if the name is a pseudonym. Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.

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 in accordance with this CPS when the Certificate issued.

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 will not be used for any functions except CA functions. In addition, end-user Subscriber Certificates cannot not be used as CA Certificates.

Participants in the DigiCert and CrossCert 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. CrossCert 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. Participants are discouraged from using the practice of “pinning” because of the difficulties that it creates on certificate roll-over and revocation events.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

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

CrossCert
7F, Halim building, Seocho Daero 320(1674-4, SeochoDong)
Seocho-gu, Seoul, 137-725 Korea

Attn: Practices Development - CPS
CrossCert Tel: +82-2-3019-5500
CrossCert Fax: +82-2-3019-5656
sm@crosscert.com

1.5.2. Contact Person

The Certificate Policy Manager / Security Manager
DigiCert Policy Authority
CrossCert

CrossCert
7F, Halim building, Seocho Daero 320(1674-4, SeochoDong)
Seocho-gu, Seoul, 137-725 Korea

Attn: Practices Development - CPS
CrossCert Tel: +82-2-3019-5500
CrossCert Fax: +82-2-3019-5656
sm@crosscert.com

1.5.2.1. Revocation Reporting Contact Person

Attn: CrossCert Technical Support
7F, Halim building, Seocho Daero 320(1674-4, SeochoDong)
Seocho-gu, Seoul, 137-725 Korea
CrossCert Tel: +82-2-3019-5500
CrossCert Fax: +82-2-3019-5656

To request that a Certificate be revoked, please email ps@crosscert.com.

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

1.5.3. Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CPS 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. CPS Approval Procedures

The DCPA approves the CPS and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with the CP, by either updating the entire CPS or by

publishing an addendum. The DCPA determines whether an amendment to this CPS is consistent with the 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

“Applicant” means an entity applying for a Certificate.

“Application Software Vendor” means a software developer whose software displays or uses CrossCert Certificates and distributes DigiCert’s root Certificates.

“CAB Forum” is defined in section 1.1.

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

“Direct Address” means an email address conforming to the Applicability Statement for Secure Health Transport.

“Direct Address Certificate” means a Certificate containing an entire Direct Address.

“Direct Organizational Certificate” means a Certificate containing only the domain name portion of a Direct Address.

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

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

“OCSP Responder” means an online software application operated under the authority of CrossCert 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.

“Qualified Certificate” means a Certificate that meets the requirements of EU law and is provided by an Issuer CA meeting the requirements of EU law.

“Relying Party” means an entity that relies upon either the information contained within a Certificate.

“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 CrossCert’s Repository. The Relying Party Agreement is available for reference through a CrossCert online repository.

“Subscriber” means the entity identified as the subject in the Certificate.

“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 for Certification Authorities.

“WHOIS” Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website.

1.6.2. Acronyms

AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	”CA/Browser” as in “CAB Forum”
CMS	Card Management System
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As (also known as "Trading As")
DCPA	DigiCert Policy Authority
DNS	Domain Name Service
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
FTP	File Transfer Protocol
GLEIF	Global Legal Entity Identifier Foundation
HISP	Health Information Service Provider
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IDN	Internationalized Domain Name
ISSO	Information System Security Officer
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
IV	Individual Validated
LEI	Legal Entity Identifier
MICS	Member-Integrated Credential Service (IGTF)
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Healthcare (U.S.)
OSU	Online Sign-Up (Wi-Fi Alliance Hotspot 2.0)
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
RA	Registration Authority

RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TTL	Time To Live
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:

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

DirectTrust Community X.509 Certificate Policy, v.1.3

Mozilla Root Store Policy v.2.7

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

CrossCert makes its CPS, Relying Party Agreements, and standard Subscriber Agreements, revocation data for issued digital Certificates available in public repositories. CrossCert develops, implements, enforces, and annually updates this CPS to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. These updates also describe how the latest version of the Baseline Requirements is implemented. As Baseline Requirements are updated, DigiCert and CrossCert review the changes to determine their impact on these practices. Each section impacted by the Baseline Requirements will be updated and provided to the DCPA for approval and implementation.

CrossCert's legal repository for most services is located at https://www.crosscert.com/repository/. CrossCert's issued Certificates and its CRLs and OCSP responses are regularly accessible online with systems described in Section 5 to minimize downtime.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The CrossCert certificate services and the repository are accessible through several means of communication:

1. On the web: https://www.crosscert.com (and via URIs included in the certificates themselves)
2. By email to sm@crosscert.com
3. By mail addressed to: CrossCert, Inc., 7F, Halim building, Seocho Daero 320(1674-4, SeochoDong), Seocho-gu, Seoul, 137-725 Korea
4. By telephone Tel: +82-2-3019-5500
5. By fax: +82-2-3019-5656

2.3. TIME OR FREQUENCY OF PUBLICATION

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least every 6 months, and also within 24 hours if a CA Certificate is revoked. Under special circumstances, CrossCert may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

For Certificates subject to the Baseline Requirements, CRLs for end-user Subscriber Certificates are issued at least once every seven days. CRLs for CAs that only issue CA Certificates subject to the Baseline Requirements are generally issued at least 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.

New or modified versions of this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

For S/MIME, Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards except that CrossCert may issue a Level 1 Certificate with a null subject DN if it includes at least one alternative name form that is marked critical. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

3.1.2. Need for Names to be Meaningful

CrossCert uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. CrossCert only allows directory information trees that accurately reflect organization structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, CrossCert does not issue anonymous or pseudonymous Certificates. CrossCert may also issue other pseudonymous end-entity Certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

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 is enforced as follows:

Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.

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 all Certificates, unless otherwise specifically stated in this CPS, CrossCert does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. CrossCert may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2. INITIAL IDENTITY VALIDATION

CrossCert may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. CrossCert 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

S/MIME Certificates issued as Level 1-2 Client Certificates.	CrossCert verifies an individual's or organization's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing the following: by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address.

For each IP Address listed in a Certificate, CrossCert confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;
2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;
4. After July 31, 2019, CrossCert will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;
5. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;
6. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or
7. Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

CrossCert uses a documented internal process to check the accuracy of information sources and databases to ensure the data is acceptable, including reviewing the database provider's terms of use.

CrossCert uses data from databases and information sources after CrossCert determines that the sources are:

- not self-reported; and
- the database or the information sources that demonstrate transparent efforts and reported methods to be accurate which can then be verified by CrossCert through analysis of the resource against other known reliable resources.

For Legal Entity Identifier (LEI) numbers listed in Certificates, CrossCert may include the value after verification, through the appropriate mechanism, such as mechanisms provided by Global Legal Entity Identifier Foundation (GLEIF), that the LEI is associated with entity information provided. LEI lookups are treated as an information from a source described above, but not currently relied upon as a primary source of information for verification. Instead, this information is treated as additional correlation of identity information found in the certificate and provided in the

certificate for the convenience and use of data researchers and the legal entities operating the certificates.

3.2.3. Authentication of Individual Identity

If a Certificate will contain the identity of an individual, then CrossCert or an RA validates the identity of the individual using the following procedures:

Certificate	Validation
Authentication-Only Certificates	The entity controlling the secure location must represent that the certificate holder is authorized to access the location.
Level 1 Client Certificates – Personal (email Certificates)[1]	As specified in Section 3.2.2 (no identity verification other than control of the email address listed in the Certificate).
Level 1 Client Certificates – Enterprise (email certificates)	Any one of the following: 1. In-person appearance before a person performing identity proofing for a Registration Authority or a 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: a. the ability to place or receive calls from a given number; or b. 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: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receives phone calls at a phone number used in previous business transactions. 4. Any method used to verify the identity of an Applicant for a Level 2 Client Certificate.
Level 2 Client Certificates	The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual: (a) the name on the government-issued photo-ID referenced below; (b) date of birth; and

[1] CrossCert and its subordinate Issuer CAs do not delegate validation of the domain portion of an e-mail address in S/MIME certificates. CrossCert and the subordinate Issuer CAs may rely upon validation the root CA has performed for an Authorized Domain Name as being valid domain names. If CrossCert is verifying the domain portion, then CrossCert will use a process the CA/B Forum authorized to meet this requirement as listed in this section.

	(c) current address or personal telephone number. 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID. 2. The Applicant must possess a valid, current, government-issued, photo ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks with an agent/institution or through credit bureaus or similar databases. CrossCert or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by 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 available to CrossCert or the RA. 3. Where CrossCert or an RA has a current and ongoing relationship with the Applicant, identity may be verified through the 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) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.

If 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 of the same type 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.

3.2.3.1. Authentication for Role-based Client Certificates

CrossCert may issue Certificates that identify a specific role that the Subscriber holds, if 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. CrossCert only issues 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. CrossCert may issue Certificates with the same role to multiple Subscribers. However, CrossCert requires 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.

CrossCert verifies the identity of the individual requesting a role-based Certificate (the sponsor) in accordance with Section 3.2.3 before issuing a role-based Certificate. The sponsor must hold a CrossCert-issued client individual Certificate at the same or higher assurance level as the role-based Certificate.

Regarding the issuance of role-based Certificates, this CPS requires compliance with all provisions of DigiCert's CP regarding key generation, private key protection, and Subscriber obligations.

3.2.3.2. Authentication for Group Client Certificates

Group Certificates correspond to a Private Key that is shared by multiple Subscribers, and are issued for allowed programs (if several entities are acting in one capacity and if non-repudiation is not required). Direct Address Certificates and Direct Organizational Certificates are used as group Certificates consistent with applicable requirements of the Direct Program. CrossCert or the RA records the information identified in Section 3.2.3 for a sponsor before issuing a group Certificate. The sponsor must be at least an Information Systems Security Officer (ISSO) or of the equivalent rank or greater within the organization.

The sponsor is responsible for ensuring control of the Private Key. The sponsor must maintain and continuously update a list of Subscribers with access to the Private Key and account for the time period during which each Subscriber had control of the key. Group Certificates may list the identity of an individual in the subjectName DN provided that the subjectName DN field also includes a text string, such as "Direct Group Cert," so that the Certificate specifies the subject is a group and not a single individual. Client Certificates issued in this way to an organization are always considered group client Certificates.

3.2.3.3. Authentication of Devices with Human Sponsors

Not applicable.

3.2.4. Non-verified Subscriber Information

The common name of a Level 1 - Personal Client Certificates is not verified as the legal name of the Subscriber. Any other non-verified information included in a Certificate is designated as such in the Certificate. Unverified information is never included in a Level 2 Certificate. OU information is generally not verified except where verification is required by industry standards.

3.2.5. Validation of Authority

The authorization of a certificate request is verified as follows:

Certificate	Verification
Level 1 Client Certificates Personal (email Certificates) and Enterprise (email Certificates)	The authority of the request is verified through 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.
Client Certificates Level 2 Certificates	The organization named in the Certificate confirms to CrossCert or an RA that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.

An organization may limit who is authorized to request Certificates by sending a request to CrossCert. A request to limit authorized individuals is not effective until approved by CrossCert. CrossCert will respond to an organization's verified request for CrossCert's list of its authorized requesters.

3.2.6. Criteria for Interoperation

Interoperation with DigiCert and CrossCert PKI is permitted pursuant to the DigiCert CP.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, CrossCert creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, CrossCert may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
Level 1 Client Certificates	Username and password or a challenge phrase	At least every nine years
Level 2 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3 or a challenge phrase	At least every nine years
Authentication-Only Certificates	Username and password or with associated Private Key	None

CrossCert does not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial registration process prior to rekeying the Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

CrossCert or an RA authenticates all revocation requests. CrossCert may authenticate revocation requests by referencing 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

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to CrossCert.

Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The Certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

CrossCert does not issue Certificates to entities on a government denied list maintained by the Republic of Korea or that is located in a country with which the laws of the Republic of Korea prohibit doing business.

4.1.2. Enrollment Process and Responsibilities

In no particular order, the enrollment process includes:

1. Submitting a certificate application;
2. Generating a Key Pair;
3. Delivering the Public Key of the Key Pair to CrossCert;
4. Agreeing to the applicable Subscriber Agreement; and
5. Paying any applicable fees.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After receiving a certificate application, CrossCert or an RA verifies the application information and other information in accordance with Section 3.2.

CrossCert 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.

If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to CrossCert. After verification is complete, CrossCert evaluates the corpus of information and decides whether or not to issue the Certificate. As part of this evaluation, CrossCert checks the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

4.2.2. Approval or Rejection of Certificate Applications

CrossCert rejects any certificate application that CrossCert or an RA cannot verify. CrossCert does not issue Certificates containing a new gTLD under consideration by ICANN until the gTLD has been approved. CrossCert may also reject a certificate application if CrossCert believes that issuing the Certificate could damage or diminish CrossCert's reputation or business.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, CrossCert will approve the certificate application and issue the Certificate. CrossCert is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

Under normal circumstances, CrossCert verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. CrossCert will usually complete the validation process and issue or reject a certificate application within two working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of CrossCert can delay the issuance process.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

CrossCert confirms the source of a certificate request before issuance. CrossCert does not issue end entity Certificates directly from its DigiCert's root Certificates. Certificate issuance by the DigiCert Root CA requires an individual authorized by DigiCert and CrossCert (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the DigiCert Root CA to perform a certificate signing operation. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

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

CrossCert may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, CrossCert delivers Certificates via email to the email address designated by the Subscriber during the application process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2. Publication of the Certificate by the CA

CrossCert publishes all CA Certificates in its repository. CrossCert publishes end-entity Certificates by delivering them to the Subscriber.

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

RAs may receive notification of a Certificate's issuance if the RA was involved in the issuance process.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate is only permitted once the Subscriber agrees to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with CrossCert's Subscriber Agreement the terms of the DigiCert CP and this CPS.

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. DigiCert does not warrant that any third party software will support or enforce the controls and requirements found herein.

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. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by CrossCert are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the CrossCert repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

CrossCert may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent, and
3. the associated Private Key remains uncompromised.

CrossCert may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. CrossCert may notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees. CrossCert 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. CrossCert may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. CrossCert will refresh any information that is older than the periods specified in the Baseline Requirements. CrossCert may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then CrossCert does not require any additional identity vetting.

4.6.4. Notification of New Certificate Issuance to Subscriber

CrossCert may deliver the Certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the Certificate.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6. Publication of the Renewal Certificate by the CA

CrossCert publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in CrossCert's repository.

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

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7. CERTIFICATE RE-KEY

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same.

4.7.1. Circumstance for Certificate Rekey

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

After re-keying a Certificate, CrossCert may revoke the old Certificate but may not further re-key, renew, or modify the previous Certificate. 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

CrossCert will only accept re-key requests from the subject of the Certificate, an authorized representative for an Organizational certificate, or the PKI sponsor. CrossCert may initiate a certificate re-key at the request of the certificate subject or at CrossCert's own discretion.

4.7.3. Processing Certificate Rekey Requests

CrossCert will only accept re-key requests from the subject of the Certificate or the PKI sponsor. If the Private Key and any identity and domain information in a Certificate have not changed, then

CrossCert can issue a replacement Certificate using a previously issued Certificate or previously provided CSR. CrossCert re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if CrossCert believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

CrossCert notifies the Subscriber within a reasonable time after the Certificate issues.

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. Issued Certificates are considered accepted 30 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

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

CrossCert publishes rekeyed Certificates by delivering them to Subscribers.

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

RAs may receive notification of a Certificate's rekey if the RA was involved in the issuance process.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances 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 CPS. The new Certificate may have the same or a different subject Public Key.

4.8.2. Who May Request Certificate Modification

CrossCert modifies Certificates at the request of certain certificate subjects or in its own discretion. CrossCert does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, CrossCert verifies any information that will change in the modified Certificate. CrossCert will only issue the modified Certificate after completing the verification process on all modified information. CrossCert will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

RAs are required to perform identification and authentication of all modified Subscriber information in terms of Section 3.2.

4.8.4. Notification of Certificate Modification to Subscriber

CrossCert notifies the Subscriber within a reasonable time after the Certificate issues.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6. Publication of the Modified Certificate by the CA

CrossCert publishes modified Certificates by delivering them to Subscribers.

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

RAs may receive notification of a Certificate's modification if the RA was involved in the issuance process.

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, CrossCert and Issuer CAs verify that the revocation request was made by either the organization or individual that made the certificate application or by an entity with the legal jurisdiction and authority to request revocation. Issuer CAs are required to provide evidence of the revocation authorization to CrossCert upon request.

4.9.1. Circumstances for Revocation

CrossCert will revoke a Certificate within 24 hours after confirming one or more of the following occurred:

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

CrossCert may revoke a certificate within 24 hours and will revoke a Certificate within 5 days after 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. CrossCert 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 the DigiCert CP, this CPS, or the relevant agreement;
4. CrossCert confirms 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. CrossCert confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. CrossCert confirms a material change in the information contained in the Certificate;
7. CrossCert confirms that the Certificate was not issued in accordance with the CA/B forum requirements or relevant browser policy;
8. CrossCert determines or confirms that any of the information appearing in the Certificate is inaccurate;

9. CrossCert's right to issue Certificates under the CA/B forum requirements expires or is revoked or terminated, unless CrossCert has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the DigiCert CP and/or this CPS; or
11. CrossCert 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.

CrossCert may revoke any Certificate in its sole discretion, including if CrossCert believes that:

1. Either the Subscriber's or CrossCert's obligations under the DigiCert CP or this 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. CrossCert received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. CrossCert ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable 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 the laws of the Republic of Korea;

CrossCert always revokes 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.

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

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies CrossCert that the original Certificate request was not authorized and does not retroactively grant authorization;
3. CrossCert 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 or any section of the Mozilla Root Store policy;
4. CrossCert obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
5. CrossCert confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. CrossCert determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. CrossCert 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. CrossCert's or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless CrossCert has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by DigiCert's Certificate Policy and/or CrossCert's 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.

CrossCert will revoke a cross-Certificate if the cross-certified entity (including CrossCert) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs 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 of 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.

4.9.3. Procedure for Revocation Request

CrossCert processes a revocation request as follows:

1. CrossCert logs the identity of entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. CrossCert may also include its own reasons for revocation in the log.
2. CrossCert may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, CrossCert revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, CrossCert personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate or website,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
5. If CrossCert determines that revocation is appropriate, CrossCert personnel revoke the Certificate and update the CRL.

If CrossCert deems appropriate, CrossCert may forward the revocation reports to law enforcement.
CrossCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. CrossCert may grant and extend revocation grace periods on a case-by-case basis. CrossCert reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

4.9.5. Time within which CA Must Process the Revocation Request

CrossCert will revoke a CA Certificate within one day after receiving clear instructions from the DCPA.

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

After reviewing the facts and circumstances, CrossCert works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which CrossCert 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 CrossCert will consider the following criteria:

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

Under normal operating circumstances, CrossCert will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking 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

DigiCert uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. For an offline CA that only issues CA Certificates, certificate-status-checking certificates, or internal administrative Certificates, CrossCert issues a CRL at least every 6 months. All other CRLs are published at least every seven days.

4.9.8. Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

CrossCert makes certificate status information available via OCSP for SSL/TLS Server Certificates. OCSP may not be available for other kinds of Certificates. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time and no later than ten seconds after the request is received, subject to transmission latencies over the Internet.

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

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are 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 contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

CrossCert supports an OCSP capability using the GET method for Certificates issued in accordance with the Baseline Requirements. OCSP Responders under CrossCert's direct control will not respond with a "good" status for a certificate that has not been issued.

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements Related to Key Compromise

CrossCert uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. CrossCert will transition any revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by an applicable CP.

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

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period, which remain on the CRL for at least 10 years following the Certificate's validity period. OCSP information for subscriber Certificates is updated at least every

four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

4.10.2. Service Availability

Certificate status services are available 24x7. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by CrossCert. CrossCert 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.

CrossCert also maintains a continuous 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

OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices

CrossCert never escrows CA Private Keys under this CPS.

CrossCert may escrow Subscriber key management keys to provide key recovery services. CrossCert encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key. Enterprise customers utilizing key escrow software provided by CrossCert may escrow keys within their or CrossCert's infrastructure.

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

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

Entities using CrossCert's key escrow services are required to:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;

4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request 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

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

CrossCert performs its CA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make CrossCert's CA operations inaccessible to non-trusted personnel. CrossCert operates under a security policy designed to detect, deter, and prevent unauthorized access to CrossCert's operations.

5.1.2. Physical Access

5.1.2.1. Data Centers

Systems providing online certificate issuance (e.g. Issuer CAs) are located in commercial data centers. CrossCert protects such online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. Access to the data centers housing the CA platforms requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card. CrossCert deactivates and securely stores its CA equipment when not in use in accordance with section 5.1.2.3. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer CrossCert's Private Keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The CrossCert data centers are continuously attended. However, if CrossCert ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, CrossCert personnel will perform a security check of the data center to verify that:

1. CrossCert's equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (e.g., door locks) are functioning properly, and
4. The area is secured against unauthorized access.

CrossCert's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.2.2. RA Operations Areas

CrossCert's RA operations are protected against access from non-authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system. The exterior and internal passageways of buildings are equipped with motion detecting sensors and video cameras. Similarly, the support and vetting rooms where CrossCert personnel perform identity vetting and other RA functions are equipped with motion-activated video surveillance cameras. Access card logs and video records are reviewed on a regular basis. CrossCert securely stores all removable media and paper containing sensitive plain-text information related to its CA or RA operations in secure containers.

5.1.2.3. Offline CA Key Storage Rooms

CrossCert securely stores the crypto modules used to generate and store offline CA Private Keys. Access to the rooms used for key storage is controlled and logged by the building access card

system. When not in use during a key ceremony, CA crypto modules are locked in a safe that provides two-person physical access control. Activation data is protected in accordance with section 6.4. Crypto module activation keys (operator cards and PED keys) are either sealed in tamper-evident bags and placed in safe deposit boxes or stored in the two-person safe when not in use. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

5.1.2.4. CA Key Generation and Signing Rooms

CA key generation and signing occurs either in the secure storage room described in section 5.1.2.3 or in a room of commensurate security in close proximity thereto. CrossCert's CA Administrators retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles.

5.1.3. Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power. CrossCert monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available.

CrossCert's data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4. Water Exposures

The cabinets housing CrossCert's CA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5. Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6. Media Storage

CrossCert protects its media from accidental damage, environmental hazards, and unauthorized physical access. Backup files are created on a daily basis. CrossCert's backup files are maintained at locations separate from CrossCert's primary data operations facility.

5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

5.1.8. Off-site Backup

CrossCert maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes located inside federally insured financial institutions and are accessible only by trusted personnel.

5.1.9. Certificate Status Hosting, CMS and External RA Systems

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

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

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. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do 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, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

5.2.1.3. System Administrators/ System Engineers (Operator)

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keep CA, CMS and RA systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if CrossCert, an Issuer CA, or RA is operating in accordance with this CPS or an RA's Registration Practices Statement.

5.2.1.5. RA Administrators

RA Administrators install, configure and manage the RA software, including the assignment of Issuer CAs and certificate profiles to customer accounts.

5.2.2. Number of Persons Required per Task

CrossCert requires that at least two people acting in a trusted role (one the CA Administrator and the other not an Internal Auditor) take action requiring a trusted role for the most sensitive tasks, such as activating CrossCert's Private Keys, generating a CA Key Pair, or backing up a CrossCert Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and
4. Those performing duties related to CA key management or CA administration.

To accomplish this separation of duties, CrossCert specifically designates individuals to the trusted roles defined in Section 5.2.1 above. CrossCert appoints individuals to only one of the Registration Officer, Administrator, Operator, or Internal Auditor roles. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. CrossCert's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

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

There is no citizenship requirement for personnel performing trusted roles associated with the issuance of other kinds of Certificates.

The CrossCert ensures that all individuals assigned to trusted roles have proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, to perform their duties under this CPS.

5.3.2. Background Check Procedures

CrossCert verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. CrossCert requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks may include a combination of the following as required; verification of individual identity, employment history, education, character references, social security number, previous residences, driving records, professional references, and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. 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 highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and re-adjudication occurs at least every five years.

These procedures are 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 by CrossCert due to a prohibition or limitation in local law, CrossCert utilizes 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. These substitutions will not be allowed for any applicant for a trusted role performing duties.

5.3.3. Training Requirements

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

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by CrossCert,
3. authentication and verification policies and procedures,
4. CrossCert 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.

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

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

5.3.4. Retraining Frequency and Requirements

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

5.3.5. Job Rotation Frequency and Sequence

Not applicable.

5.3.6. Sanctions for Unauthorized Actions

CrossCert employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of

employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

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

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

CrossCert's systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

CrossCert enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If CrossCert's applications cannot automatically record an event, CrossCert implements manual procedures to satisfy the requirements. For each event, CrossCert records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. All event records are available to auditors as proof of CrossCert's practices. Logs are maintained to the standard per the requirements of the relevant policies and programs.

CrossCert records 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, the DigiCert CP, and this 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 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

As required, generally within at least once every two months, a CrossCert administrator reviews the logs generated by CrossCert's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to CrossCert's operations management committee and are made available to CrossCert's auditors upon request. CrossCert documents any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

Audit logs in accordance with section 5.5.2. CrossCert retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from CrossCert's CA systems are different than the individuals who control CrossCert's signature keys.

5.4.4. Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. CrossCert's CA systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. CrossCert's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

Audit logs are made available to auditors upon request.

5.4.5. Audit Log Backup Procedures

CrossCert makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

Where required, CrossCert creates incremental backups of audit logs daily and full backups weekly.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end 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, CrossCert's Administrators and the DCPA shall be notified and the DCPA will consider suspending the 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

CrossCert performs annual 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. CrossCert also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that CrossCert has in place to control such risks. CrossCert's Internal Auditors review the security audit data checks for continuity. CrossCert's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. RECORDS ARCHIVAL

CrossCert complies with all record retention policies that apply by law and retrieved as necessary by request of authorized parties. CrossCert includes sufficient detail in all archived records to show that a Certificate was issued in accordance with this CPS.

5.5.1. Types of Records Archived

CrossCert retains the following information in its archives (as such information pertains to CrossCert's CA operations):

1. Accreditations of CrossCert,
2. The DigiCert CP and this CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, rekey, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a Certificate,
9. Subscriber Agreements,
10. Issued Certificates,
11. A record of certificate re-keys,
12. Data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Changes to CrossCert'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 DigiCert CP or this CPS.

5.5.2. Retention Period for Archive

CrossCert, or the RA supporting issuance, archives data for all certificates for at least 7.5 years.

5.5.3. Protection of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the DCPA or as required by law. CrossCert maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If CrossCert needs to transfer any media to a different archive site or equipment, CrossCert will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

On at least an annual basis, CrossCert creates an archive of the data listed in section 5.5.1. Each archive is stored separately and available for integrity verification at a later date. CrossCert stores the archive in a secure location for the duration of the set retention period.

5.5.5. Requirements for Time-stamping of Records

CrossCert automatically time-stamps archived records with system time (non-cryptographic method) as they are created. CrossCert synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6. Archive Collection System (internal or external)

Archive information is collected internally by CrossCert.

5.5.7. Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the CrossCert PKI, CrossCert may elect to retrieve the information from archival. The integrity of archive information is verified by comparing a hash of the archive disk with the hash originally stored for that disk, as described in Section 5.5.4. CrossCert may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6. KEY CHANGEOVER

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

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

CrossCert maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. CrossCert reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

CrossCert makes regular system backups weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location. If CrossCert discovers that any of its computing resources, software, or data operations have been compromised, CrossCert assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If CrossCert determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, CrossCert suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

If CrossCert suspects that one of its CA Private Keys has been comprised or lost then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. Specifically, CrossCert will:

1. Collect information related to the incident;
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. Make information available that can be used to identify which Certificates are affected, unless doing so would breach the privacy of a CrossCert user or the security of CrossCert's services;
6. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
7. Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;
8. Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and
9. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

CrossCert may generate a new Key Pair and sign a new Certificate. If a disaster physically damages CrossCert's equipment and destroys all copies of CrossCert's signature keys then CrossCert will provide notice to affected parties at the earliest feasible time.

5.7.4. Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, CrossCert implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving CrossCert's primary facility and that CrossCert be capable of maintaining other services or resuming them as quickly as possible following a disaster. CrossCert reviews, tests, and updates the BCMP and supporting procedures at least annually.

CrossCert's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes CrossCert's primary CA operations to become inoperative, CrossCert will re-initiate its

operations at its secondary location giving priority to the provision of certificate status information capabilities, if affected.

5.8. CA OR RA TERMINATION

Before terminating its CA activities, CrossCert will:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on CrossCert's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, CrossCert will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

CrossCert has made arrangements to cover the costs associated with fulfilling these requirements in case CrossCert becomes bankrupt or is unable to cover the costs. Any requirements of this section that are varied by contract apply only the contracting parties.

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.

CrossCert's CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-2 Level 3. Activation of the hardware requires the use of two-factor authentication tokens. CrossCert creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process. For CA key pair generation ceremonies, an Internal Auditor, external auditor, or independent third party attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

Subscribers must generate their keys in a manner that is appropriate for the certificate type.

6.1.2. Private Key Delivery to Subscriber

If CrossCert, a CMS, or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery,
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and
4. The key generator must 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.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. A CMS or RA providing key delivery services is required to provide a copy of this record to CrossCert.

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 generate Key Pairs and submit the Public Key to CrossCert in a CSR as part of the certificate request process.

6.1.4. CA Public Key Delivery to Relying Parties

CrossCert's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root

store, and/or as roots signed by other CAs. All accreditation authorities supporting CrossCert Certificates and all application software providers are permitted to redistribute DigiCert's root anchors.

CrossCert may also distribute Public Keys that are part of an updated signature Key Pair as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may obtain CrossCert's self-signed CA Certificates from CrossCert's web site or by email.

6.1.5. Key Sizes

CrossCert generally follows the NIST timelines in using and retiring signature algorithms and key sizes. Accordingly, CrossCert is phasing out its use of the SHA-1 hash algorithm.

Certificates may also be signed using the SHA-1 hash algorithm, provided that its use otherwise complies with requirements of the CA/Browser Forum, the Mozilla Root Store policy, other policies and programs listed in section 1.1 and 1.6.3, or the relevant CP. Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm if it is compliant with all applicable programs listed in section 1.1. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

CrossCert requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms.

CrossCert may require higher bit keys in its sole discretion if it is compliant with references in section 1.1 and 1.6.3.

CrossCert and Subscribers may fulfill the transmission security requirements under the DigiCert CP and this CPS 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

CrossCert uses a crypto module that conforms to FIPS 186-2 and provides random number generation and on-board generation of Public Keys and a wide range of ECC curves. The value of this public exponent equates to an odd number equal to three or more.

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

CrossCert's Certificates 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 are not 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

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

Key usage bits and extended key usages are specified in the certificate profile for each type of Certificate. CrossCert's CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

For Certificates at Levels 1, 2 that are used for signing and encryption in support of legacy applications, they must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CPS,
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.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

CrossCert's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140-2 Level 3.

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

Assurance Level	Subscriber	Registration Authority
Rudimentary	N/A	FIPS 140-2 Level 1 (Hardware or Software)
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)
Medium	FIPS 140-2 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
Medium Hardware, Biometric /Hardware Authentication	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

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

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

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

6.2.3. Private Key Escrow

CrossCert does not escrow its signature keys. Subscribers may not escrow their private signature keys. CrossCert may provide escrow services for other types of Certificates in order to provide key recovery as described in section 4.12.1.

6.2.4. Private Key Backup

CrossCert's Private Keys are generated and operated inside CrossCert's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. CrossCert's CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and video-recorded key backup process. CrossCert may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the Subscriber can control the Private Key. Backed up keys are never stored in a plain text form outside of the cryptographic module.

6.2.5. Private Key Archival

CrossCert does not archive 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. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, CrossCert encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access. If CrossCert becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then CrossCert will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If CrossCert pre-generates private keys and transfers them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, it will 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

CrossCert's Private Keys are generated and stored inside CrossCert's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3.

6.2.8. Method of Activating Private Keys

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

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

6.2.9. Method of Deactivating Private Keys

CrossCert's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. CrossCert never leaves its HSM devices in an active unlocked or unattended state.

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

6.2.10. Method of Destroying Private Keys

CrossCert personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

CrossCert may destroy a Private Key by deleting it from all known storage partitions. CrossCert also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, CrossCert will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

CrossCert archives copies of Public Keys in accordance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

CrossCert Certificates have maximum validity periods of:

Type	Private Key Use[2]	Certificate Term
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
CRL and OCSP responder signing	3 years	31 days
End Entity / Client for all other purposes	36 months	36 months

Participants shall cease all use of their key pairs after their usage periods have expired. Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

CrossCert may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. CrossCert does not issue Subscriber Certificates 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

[2] CA Private Keys may continue to be used to sign CRLs and OCSP responses.

6.4.1. Activation Data Generation and Installation

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

All CrossCert personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords that meet the requirements specified by the CAB Forums Network Security Requirements. If CrossCert uses passwords as activation data for a signing key, CrossCert will change the activation data change upon rekey of the CA Certificate.

6.4.2. Activation Data Protection

CrossCert protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All CrossCert personnel are instructed to memorize and not to write down their password or share it with another individual. CrossCert locks accounts used to access secure CA processes if a certain number of failed password attempts occur as specified in the internal security policies, procedures, and relevant requirements in references listed in Section 1.6.3.

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

Not applicable.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

CrossCert secures its CA systems and authenticates and protects communications between its systems and trusted roles. CrossCert's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

RAs must 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 must logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs must 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 must require the use of passwords .with a minimum character length and a combination of alphanumeric and special characters.

CrossCert’s CA systems are configured 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.

All Certificate Status Servers:
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.

CrossCert enforces 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

CrossCert has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. CrossCert only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by CrossCert are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to CrossCert's operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

CrossCert has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, CrossCert verifies 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

CrossCert and RA functions are performed using networks secured in accordance with the standards documented in the DigiCert 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.

CrossCert documents and controls the configuration of its systems, including any upgrades or modifications made. CrossCert's CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). CrossCert's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

CrossCert's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. CrossCert's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

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

CrossCert uses the ITU X.509, version 3 standard to construct digital Certificates for use within the CrossCert PKI. CrossCert adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. CrossCert generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

7.1.2. Certificate Extensions

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: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId, and CrossCert no longer includes both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

CrossCert's Technically Constrained Subordinate CA Certificates 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 KeyPurposeId does not appear in the EKU extension of publicly trusted certificates.

7.1.3. Algorithm Object Identifiers

CrossCert Certificates are signed using one of the following algorithms:

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption[3]	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha256[4]	[iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2]
ecdsa-with-SHA384[5]	[iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3]

CrossCert does not currently sign Certificates using RSA with PSS padding. SSL/TLS Server Certificates and OCSP Certificates are not signed with sha-1WithRSAEncryption.

CrossCert and Subscribers may generate Key Pairs using the following:

id-dsa	[iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1]

[3] Legacy applications include the following algorithm ObjectIdentifier: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

[4] Legacy applications include the following algorithm ObjectIdentifier: {iso(1) member-body(2) us(840)ansi-X9- 62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}

[5] Legacy applications include the following algorithm ObjectIdentifier: {iso(1) member-body(2) us(840)ansi-X9- 62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

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-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]
id-ecPublicKey	[iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1]

Elliptic curve Public Keys submitted to CrossCert for inclusion in end entity Certificates should all be based on NIST “Suite B” curves.

7.1.4. Name Forms

CrossCert shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 5280. CrossCert shall include a unique serial number in each Certificate. The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. The Issuer CA shall restrict OU fields from containing Subscriber information that is not verified in accordance with Section 3. 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. The commonName attribute must be present and the contents should be an identifier for the certificate such that the certificate’s Name is unique across all certificates issued by the issuing certificate.

7.1.5. Name Constraints

CrossCert may include name constraints in the nameConstraints field when appropriate.

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 includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

(a) For each dNSName in permittedSubtrees, the CrossCert confirms 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, CrossCert confirms 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 CrossCert confirms 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 specifies the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate includes within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate also includes within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate includes at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate includes a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate includes 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 also includes 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

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by CrossCert are listed in Section 1.2.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

CrossCert includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension. Those Certificates may 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

7.2.1. Version number(s)

CrossCert issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	[DigiCert or CrossCert]
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate

Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3. OCSP PROFILE

7.3.1. Version Number(s)

CrossCert's OCSP responders conform to version 1 of RFC 6960.

7.3.2. OCSP Extensions

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities as required by the Mozilla Root Store policy and other programs listed in section 1.1 and 1.6.3.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

CrossCert receives an annual period in time audit by an independent external auditor to assess CrossCert's compliance with this CPS, referenced requirements, any applicable CPs, and the WebTrust for CA programs criteria. The audit covers CrossCert's RA systems, Sub CAs, and OCSP Responders.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

The audit covers CrossCert's business practices disclosure, the integrity of CrossCert's PKI operations, and CrossCert's compliance with this CPS and referenced requirements. The audit verifies that CrossCert is compliant with the DigiCert CP, this CPS, and any MOA between it and any other PKI.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CPS, the DigiCert CP, or any other contractual obligations related to CrossCert's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify CrossCert, and (3) CrossCert will develop a plan to cure the noncompliance. CrossCert will submit the plan to the DCPA for approval and to any third party that CrossCert 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. CrossCert is entitled to suspend and/or terminate of 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 are reported to the DCPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of CrossCert's WebTrust for CAs audit reports can be found at: https://www.crosscert.com. On an annual basis and within three months of completion, DigiCert submits copies of relevant audit compliance reports to various parties, such as Mozilla, Adobe, CA licensing bodies, etc.

8.7. SELF-AUDITS

On at least a quarterly basis, CrossCert performs regular internal audits against a randomly selected sample of at least three percent of its Certificates issued since the last internal audit. Self-audits are performed in accordance with Guidelines adopted by the CA / Browser Forum.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

CrossCert charges fees for certificate issuance and renewal. CrossCert may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

CrossCert does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL.

CrossCert may charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. CrossCert does not permit access to revocation information, Certificate status information in their repositories by third parties that provide products or services that utilize such Certificate status information without CrossCert's prior express written consent.

9.1.4. Fees for Other Services

CrossCert does not charge a fee for access to this 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

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

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

CrossCert maintains Professional Liability/Errors & Omissions insurance with a policy limit of $2 million in coverage. Insurance is carried through companies 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

CrossCert provides a limited warranty to Relying Parties in CrossCert's Relying Party Agreement.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

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

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by CrossCert as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2. Information Not Within the Scope of Confidential Information

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

9.3.3. Responsibility to Protect Confidential Information

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

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

DigiCert follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws.

9.4.2. Information Treated as Private

CrossCert treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. CrossCert protects private information using appropriate safeguards and a reasonable degree of care.

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

DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements of applicable local privacy laws concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

CrossCert may disclose private information, without notice, if DigiCert believes the disclosure is required by law or regulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

The allocation of Intellectual Property Rights among CrossCert Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such CrossCert Sub-domain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1. Property Rights in Certificates and Revocation Information

CrossCert retains all intellectual property rights in and to the Certificates and revocation information that they issue. CrossCert 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. CrossCert, 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 CrossCert retains all intellectual property rights in and to this CPS.

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 CrossCert 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

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, CrossCert does not make any representations regarding its products or services. CrossCert represents, to the extent specified in this CPS, that:

1. CrossCert complies, in all material aspects, with the DigiCert CP, this CPS, and all applicable laws and regulations,
2. CrossCert publishes and updates CRLs and OCSP responses on a regular basis,
3. All Certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the Baseline Requirements, and
4. CrossCert will maintain a repository of public information on its website.

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

9.6.2. RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to the DigiCert CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All Certificates requested by the RA meet the requirements of this CPS.

CrossCert's agreement with the RA may contain additional representations.

Subscriber Agreements may include additional representations and warranties.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify CrossCert and any applicable RA if a change occurs that could affect the status of the Certificate.

CrossCert 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 CrossCert and the Certificate Beneficiaries.
Prior to the issuance of a Certificate, CrossCert will obtain, for the express benefit of CrossCert and the Certificate Beneficiaries, either:

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

Subscribers represent to CrossCert, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with CrossCert,
3. Confirm the accuracy of the 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 CrossCert 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. 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

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

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

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

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 IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. CROSSCERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT

ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.8. LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM CROSSCERT'S NEGLIGENCE OR (II) FRAUD COMMITTED BY CROSSCERT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A CROSSCERT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF CROSSCERT RELATED TO SUCH USE, PROVIDED THAT CROSSCERT HAS MATERIALLY COMPLIED WITH THIS CPS IN PROVIDING THE CERTIFICATE OR SERVICE. CROSSCERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS SET FORTH IN THE NETSURE EXTENDED WARRANTY PROTECTION PLAN AND THE CROSSERT RELYING PARTY AGREEMENT.

All liability is limited to actual and legally provable damages. CrossCert is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if CrossCert is aware of the possibility of such damages;
2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CPS;
4. Liability related to the security, usability, or integrity of products not supplied by CrossCert, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether CrossCert failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of CrossCert's Certificates and services.

To the extent CrossCert has issued and managed the Certificate(s) at issue in compliance with its CPS, CrossCert 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 CrossCert'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 CrossCert

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

To the extent permitted by law, each Subscriber shall indemnify CrossCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3. Indemnification by Relying Parties

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

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

CrossCert accepts notices related to this CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from CrossCert. 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. CrossCert may allow other forms of notice in its Subscriber Agreements.

CrossCert will notify Mozilla if:

1. Ownership or control of the CA certificates 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 CrossCert's included certificate(s);
3. Ownership or control of CrossCert's operations changes; or
4. There is a material change in CrossCert'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

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

9.12.2. Notification Mechanism and Period

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

9.12.3. Circumstances under which OID Must Be Changed

The DCPA is solely responsible for determining whether an amendment to the CPS requires 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 CrossCert, the procedure to resolve disputes involving CrossCert require an initial negotiation period of sixty (60) days followed by litigation in court of CrossCert jurisdiction, in the case of claimants who are Korea 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

Parties are required to notify CrossCert and attempt to resolve disputes directly with CrossCert before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

The laws of the Republic of Korea govern the interpretation, construction, and enforcement of this CPS and all proceedings related to CrossCert's products and services, including tort claims, without regard to any conflicts of law principles. The Korea, has non-exclusive venue and jurisdiction over any proceedings related to the CPS or any CrossCert product or service.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations, including Republic of Korea restrictions on the export of software and cryptography products. CrossCert shall meet the requirements of PERSONAL INFORMATION PROTECTION ACT in Republic of Korea 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

CrossCert contractually obligates each RA to comply with this CPS and applicable industry guidelines. CrossCert also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of CrossCert. Unless specified otherwise in a contact with a party, CrossCert does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

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

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

9.16.5. Force Majeure

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

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

9.17. OTHER PROVISIONS

No stipulation.