

# InCommon Certification Practices Statement

for

## Code Signing~~Server~~ Certificates

7 June 2011  
~~16 August 2010~~  
Version 1.0

Latest version:

7 June 2011[https://www.incommon.org/cert/repository/cps\\_ssl.pdf](https://www.incommon.org/cert/repository/cps_ssl.pdf)

This version:

7 June 2011[https://www.incommon.org/cert/repository/cps\\_ssl\\_20100816.pdf](https://www.incommon.org/cert/repository/cps_ssl_20100816.pdf)

1.1.1.1 TABLE OF CONTENTS

## **Table of Contents**

1 INTRODUCTION.....	4
1.1 Overview.....	4
1.2 Document Name and Identification.....	4
1.3 PKI Participants.....	5
1.4 Certificate Usage.....	5
1.5 Policy Administration.....	6
1.6 Definitions and Acronyms.....	6
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	8
2.1 Repositories.....	8
2.2 Publication of Certification Information.....	8
2.3 Time or Frequency of Publication.....	8
2.4 Access Controls on Repositories.....	8
3 IDENTIFICATION AND AUTHENTICATION.....	9
3.1 Naming.....	9
3.2 Initial Identity Validation.....	10
3.3 Identification and Authentication for Re-key Requests.....	11
3.4 Identification and Authentication for Revocation Request.....	11
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	11
4.1 Certificate Application.....	11
4.2 Certificate Application Processing.....	12
4.3 Certificate Issuance.....	12
4.4 Certificate Acceptance.....	12
4.5 Key Pair and Certificate Usage.....	12
4.6 Certificate Renewal.....	13
4.7 Certificate Re-key.....	13
4.8 Certificate Modification.....	14
4.9 Certificate Revocation and Suspension.....	14
4.10 Certificate Status Services.....	15
4.11 End of Subscription.....	16
4.12 Key Escrow and Recovery.....	16
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	16
5.1 Physical Controls.....	16
5.2 Procedural Controls.....	17
5.3 Personnel Controls.....	17
5.4 Audit Logging Procedures.....	18
5.5 Records archival.....	19
5.6 Key changeover.....	19
5.7 Compromise and disaster recovery.....	19
5.8 CA or RA termination.....	19
6 TECHNICAL SECURITY CONTROLS.....	19
6.1 Key pair generation and installation.....	20
6.2 Private Key Protection and Cryptographic Module Engineering Controls.....	20

6.3 Other aspects of key pair management.....	21
6.4 Activation data.....	21
6.5 Computer security controls.....	22
6.6 Life cycle technical controls.....	22
6.7 Network security controls.....	22
6.8 Time-stamping.....	22
7 CERTIFICATE, CRL, AND OCSP PROFILES.....	22
7.1 Certificate profile.....	22
7.2 CRL profile.....	23
7.3 OCSP profile.....	23
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	24
8.1 Frequency or Circumstances of Assessment.....	24
8.2 Identity/Qualifications of Assessor.....	24
8.3 Assessor's Relationship to Assessed Entity.....	24
8.4 Topics Covered by Assessment.....	24
8.5 Actions Taken as a Result of Deficiency.....	24
8.6 Communication of Results.....	24
9 OTHER BUSINESS AND LEGAL MATTERS.....	24
9.1 Fees.....	24
9.2 Financial Responsibility.....	25
9.3 Confidentiality of Business Information.....	25
9.4 Privacy of Personal Information.....	25
9.5 Intellectual Property Rights.....	26
9.6 Representations and Warranties.....	27
9.7 Disclaimers of Warranties.....	27
9.8 Limitations of Liability.....	27
9.9 Indemnities.....	27
9.10 Term and Termination.....	28
9.11 Individual notices and Communications with Participants.....	28
9.12 Amendments.....	28
9.13 Dispute Resolution Provisions.....	28
9.14 Governing Law.....	29
9.15 Compliance with Applicable Law.....	29
9.16 Miscellaneous Provisions.....	29
9.17 Other Provisions.....	29
.....	30

## 1 INTRODUCTION

InCommon (“InCommon”) is an identity and trust community and services provider that offers optional subscription services for X.509 PKI certificates issued by an InCommon certification authority. Subscribers are institutions as defined in the InCommon Cert Services website ([incommon.org/cert](http://incommon.org/cert)). InCommon verifies the identity of each Subscriber and the Internet domains for which they are authoritative. InCommon outsources functions associated with public key operations which include receiving certificate signing requests, requests for revoking and renewing digital certificates, and the maintenance, issuance, and publication of Certificate Revocation Lists (“CRLs”) and the operation of an Online Certificate Status Protocol (“OCSP”) responder.

### 1.1 Overview

This InCommon Certification Practices Statement (CPS) outlines the legal, commercial, and technical principles and practices InCommon employs in approving, issuing, and managing its certificate services under the Intermediary CA Agreement (“Comodo Agreement”) between Comodo CA Limited (“Comodo”) and University Corporation for Advanced Internet Development (d/b/a Internet2) and its single-member LLC, InCommon. Under this agreement, Comodo provides full operational support, under its own CPS, for a CA that is subordinate to the Comodo “AddTrust External CA.” This CA signs end-user certificates for entities authenticated by subscribing institutions. Subscribing institutions will take appropriate technical and non-technical means to ensure that only properly identified entities are issued certificates.SSL/TLS certificates as a result of Certificate Signing Requests (CSRs) approved by InCommon designated representatives (and their delegates) of research or educational institutions that are Subscribers to the InCommon Server CA service. InCommon’s sole responsibilities are to

InCommon’s sole responsibilities are to verify which Internet domain names may be asserted in SSL/TLS certificates requested by a subscribing institution;

- verify the identity of the subscribing institution;
- identify specific individuals at the institution who will be responsible for how certificates will be requested; and
- ensuring that subscribing institutions abide by the terms of their Subscriber Agreement with InCommon.

The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647. To preserve the format of RFC 3647, some section headings do not apply and will contain the text “Not applicable” (“n/a”) or “No stipulation”. The RFC 3647 format is preserved to assist the reader in comparing and contrasting the various CPS documents provided by various CAs.

Sections of this CPS refer to services or practices provided by Comodo under the Comodo Agreement and in accord with provisions with the Comodo AddTrust External CA “Certification Practice Statement” (<http://www.comodo.com/about/comodo-agreements.php>). Such sections will contain the text “Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.” The phrase “issued by InCommon” is to be interpreted as “issued by the Comodo CA under the Comodo Agreement.”

### 1.2 Document Name and Identification

This document is the InCommon Code Signing Certificate CPS version 1.0, which was approved for publication on 7 June 2011PS version 1.0, which was approved for publication on July 19 2010 by InCommon's certification Policy Authority. There is no separate Certification Policy document; policy is incorporated within this document.

The object identifier (cpOID) for this CPS is identified in Appendix B and will be included in end-entity certificates issued by InCommon. The current version of the CPS is made available to the public through InCommon's repository as described in Section 2 below.

Revisions not deemed significant by InCommon's Policy Authority have minimal or no impact on subscribers and relying parties using certificates, the CRLs, or the OCSP responder. Insignificant revisions may be made without changing the version number of the CPS.

Revisions that are deemed significant or may affect the use or trustworthiness of certificates will result in assignment of a new cpOID to this document.

Revisions to this document have been made as follows:

<b>Date</b>	<b>Changes</b>	<b>Version</b>
-------------	----------------	----------------

---

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

Certification authorities issue public key certificates to subscribers. A certification authority:

- Conforms its operations to this CPS as amended,
- Revokes certificates upon request by an authorized person,
- Maintains and updates its OCSP on a regular basis,
- Publishes CRLs on a regular basis,
- Distributes issued certificates, and
- Notifies subscribers via email of expiring certificates that it has issued to them.

### 1.3.2 Registration Authorities

InCommon manages its own Registration Authority (RA). Each Subscriber organization also manages and operates a delegated RA – comprising its Subscriber Registrars and any Delegated Subscriber Registrars – that is responsible for activities under its own management control for its own organization.

### 1.3.3 Subscribers

Subscribers are research and education institutions, organizations, or other entities that use InCommon's PKI services to acquire certificates that support transactions and communications.

Subjects are identified in an issued certificate. The Requester controls the private key corresponding to the public key listed in an issued certificate.

Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

### 1.3.4 Relying Parties

Relying parties use InCommon's PKI service certificates to perform transactions, communications, or other functions at their own discretion.

Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be ~~ethical~~ ~~an ethical business operation~~. It is the Relying Parties' responsibility to independently examine each certificate holder to determine whether the certificate owner is ethical and trustworthy.

## 1.4 Certificate Usage

A digital certificate is formatted data that cryptographically binds an identified Subject to a public key. A digital certificate allows an entity taking part in an electronic transaction to assert its identity to the other participants in such a transaction. Certificates ~~will only be issued to end users under this CPS. may be issued for individuals, organizations, government entities, educational institutions, or infrastructure components such as firewalls, routers, or other security devices.~~

### 1.4.1 Appropriate Certificate Uses

Depending on the certificate type, the certificates issued from an InCommon CA may be used for authentication, encryption, access control, and digital signature purposes.

### 1.4.2 Prohibited Certificate Uses

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations including export laws as described in the Subscriber Addendum. Certificates may not be used to complete or assist in performing any transaction that is prohibited by law. Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be ~~ethical~~an ethical business operation.

Certificates may not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause loss of life or property.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

This CPS is administered by the InCommon Policy Authority (PA). The InCommon PA is described in a document available in the InCommon CA repository as described in Section 2.

### 1.5.2 Contact Person

InCommon:

~~John Krienke~~

Chief Operating Officer, InCommon

c/o Internet2

1000 Oakbrook Dr, Suite 300

Ann Arbor, MI 48104~~3~~

Email: [incommon-admin@incommonfederation.org](mailto:incommon-admin@incommonfederation.org)

Phone: 734.913.4250~~352-7095~~

### 1.5.3 Person Determining CPS Suitability for the Policy

There is no separate Certificate Policy document. The CPS combines both policy and practices.

### 1.5.4 CPS Approval Procedures

InCommon's CPS (and any amendments made to it) are reviewed and approved by InCommon's Policy Authority with concurrence from its legal adviser and from Comodo. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum.

## 1.6 Definitions and Acronyms

### Acronyms:

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	PKCS#10 Certificate Signing Request
MDC	Multiple Domain Certificate
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority

- SGC Server Gated Cryptography
- SSL Secure Sockets Layer
- TLS Transaction Layer Security
- URL Uniform Resource Locator
- X.509 The ITU-T standard for Certificates and their corresponding authentication framework

**Definitions:**

<u>Applicant</u>	<u>The entity applying to become a Subscriber to the InCommon PKI services. May also be used to refer to an individual submitting a request for a certificate (see Requester below).</u>
<u>Certificate</u>	<u>A message that, at least, states a name or identifies the CA, identifies the Subject, contains the Subject's public key, and contains a serial number.</u>
<u>Delegated Subscriber Registrar</u>	<u>Any other individual to whom the Subscriber Registrar sub-delegates his or her permissions.</u>
<u>Master Registrar</u>	<u>Individuals within InCommon's Registration Authority who can delegate authority for certain Internet domains to up to 3 individuals within a Subscriber organization.</u>
<u>Registration Authority</u>	<u>The InCommon officer(s) who identify Subscriber Registrars and vet the Internet domains for which Subscriber may issue CSRs.</u>
<u>Registrar</u>	<u>The generic term for an individual who may approve submittal of a CSR to the CA and has certain privileges to manage the certificate life cycle. Master Registrar, Subscriber Registrar and Delegated Subscriber Registrar are collectively Registrars and individually a Registrar.</u>
<u>Relying Party</u>	<u>An entity that relies upon the information contained within the Certificate.</u>
<u>Relying Party Agreement</u>	<u>An agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the InCommon PKI repository as described in Section 2.</u>
<u>Requester</u>	<u>An individual who submits a CSR either via the Comodo User Interface (UI) or indirectly via the Comodo Application Programming Interface (API).</u>
<u>Subject</u>	<u>The entity that has been named in a Certificate.</u>
<u>Subscriber</u>	<u>An entity that has entered into an agreement with InCommon to make use of InCommon PKI services.</u>
<u>Subscriber Addendum</u>	<u>A legal addendum to the InCommon Participation Agreement that must be read and accepted by an Applicant before becoming a Subscriber. The Subscriber Addendum binds the Subscriber and all agents of the Subscriber that manage or acquire certificates from InCommon to its terms and conditions.</u>
<u>Subscriber Executive</u>	<u>The management officer at the Subscribing organization responsible for designating the organization's Subscriber Registrars. The Executive is authorized as such in the InCommon participation agreement or by succession and is typically be filled by a CIO, VP of IT, or other senior administrative officer responsible for</u>

	<u>the organization's information technology assets.</u>
<u>Subscriber Registrar</u>	<u>An individual that the Subscriber's executive contact identifies to InCommon and InCommon registers with Comodo and provides credentials to allow approval of CSRs on behalf of Subscriber. A Subscriber Registrar may delegate his or her permissions to another individual whom the institution wishes to allow to approve certificate requests and manage certificate lifecycle generally. Credentials may also be installed in an automated system for the issuance of end-entity certificates.</u>
<u>Applicant</u>	<u>The entity applying to become a Subscriber to the InCommon PKI services. May also be used to refer to an individual submitting a request for a certificate (see Requester below).</u>
<u>Certificate</u>	<u>A message that, at least, states a name or identifies the CA, identifies the Subject, contains the Subject's public key, and contains a serial number.</u>
<u>Delegated Subscriber Registrar</u>	<u>Any other individual to whom the Subscriber Registrar sub-delegates his or her permissions.</u>
<u>Master Registrar</u>	<u>Individuals within InCommon's Registration Authority who can delegate authority for certain Internet domains to up to 3 individuals within a Subscriber organization.</u>
<u>Registration Authority</u>	<u>The InCommon officer(s) who identify Subscriber Registrars and vet the Internet domains for which Subscriber may issue CSRs.</u>
<u>Registrar</u>	<u>The generic term for an individual who may approve submittal of a CSR to the CA and has certain privileges to manage the certificate life cycle. Master Registrar, Subscriber Registrar and Delegated Subscriber Registrar are collectively Registrars and individually a Registrar.</u>
<u>Relying Party</u>	<u>An entity that relies upon the information contained within the Certificate.</u>
<u>Relying Party Agreement</u>	<u>An agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the InCommon PKI repository as described in Section 2.</u>
<u>Requester</u>	<u>An individual who submits a CSR either via the Comodo User Interface (UI) or indirectly via the Comodo Application Programming Interface (API).</u>
<u>Subject</u>	<u>The entity that has been named in a Certificate.</u>
<u>Subscriber</u>	<u>An entity that has entered into an agreement with InCommon to make use of InCommon PKI services.</u>
<u>Subscriber Addendum</u>	<u>A legal addendum to the InCommon Participation Agreement that must be read and accepted by an Applicant before becoming a Subscriber. The Subscriber Addendum binds the Subscriber and all agents of the Subscriber that manage or acquire certificates from InCommon to its terms and conditions.</u>
<u>Subscriber Executive</u>	<u>The management officer at the Subscribing organization responsible for designating the organization's Subscriber Registrars. The Executive is authorized as such in the InCommon participation agreement or by succession and is typically be filled by a CIO, VP of IT, or other senior administrative officer responsible for</u>

Subscriber Registrar

the organization's information technology assets.

An individual that the Subscriber's executive contact identifies to InCommon and InCommon registers with Comodo and provides credentials to allow approval of CSRs on behalf of Subscriber. A Subscriber Registrar may delegate his or her permissions to another individual whom the institution wishes to allow to approve certificate requests and manage certificate lifecycle generally.

## 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CPS is only one of a set of documents relevant to InCommon's certificate services. The list of documents below is a non-exhaustive list of other relevant documents. The document name, location of, and status, whether public or private, are detailed below.

Document Status Location	Status	Location
<a href="#">InCommon Code Signing Certification Practices Statement (This document)</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">InCommon Certificate Service Subscriber Addendum and InCommon Participation Agreement</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">InCommon Certificate Service Relying Party Agreement</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">InCommon Policy Authority</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">Code signingCA and Certificate Profiles</a>	Public	<a href="#">InCommon Repository</a>

  

Document Status Location	Status	Location
<a href="#">InCommon Certification Practice Statement (This document)</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">SSL Subscriber Agreement</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">SSL Relying Party Agreement</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">InCommon Policy Authority</a>	Public	<a href="#">InCommon Repository</a>
<a href="#">SSL CA and Certificate Profiles</a>	Public	<a href="#">InCommon Repository</a>

### 2.1 Repositories

InCommon publishes this CPS, related documents and certificates in its PKI services repository at <https://www.incommon.org/cert/repository/>. The InCommon Operations group maintains the repository. InCommon makes reasonable efforts to ensure that the information in its repository is accurate, updated, and correct. However, in no event shall InCommon be liable for any amounts beyond the limits set forth in this CPS.

Parties accessing the repository agree to the terms posted in the repository in regard to its use of the documents and information on the repository. InCommon may revoke repository privileges for any party failing to comply with the terms on InCommon's website.

### 2.2 Publication of Certification Information

Certificate information is published in accordance with the provisions of the CPS relevant to such a certificate. Certificate content is published by issuing the certificate. Revoked certificate information is published in CRLs by InCommon's CA service provider and is available also by OCSP. Users and relying parties should consult the CRLs or OCSP server prior to relying on information featured in a certificate.

## 2.3 Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12. Updates to the Subscriber Agreement, Relying Party Agreements, and other agreements posted in the repository are published as often as necessary. Certificates are published upon issuance.

## 2.4 Access Controls on Repositories

The information published in the InCommon repository (refer to section 2.1) is public information and may be accessed freely by anyone visiting the site, provided they agree to the site's terms and conditions as posted thereon. Read-only access to the information is unrestricted except as stated in section 2.1 above. InCommon has implemented logical and physical security measures to prevent unauthorized additions, modification, or deletions of repository entries.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of Names

InCommon Certificates are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields. Issuer Distinguished Names will identify Internet2 (InCommon's parent organization) as the primary organization and InCommon as the organizational unit and common name. Certificate Subject Distinguished Names will identify the Subscriber as the primary organizational unit and optionally may contain an organizational subordinate unit. The Subject will be in a name space owned by or under the administrative control of the Subscriber [Institution which requested the issuance of the code signing certificate.](#)<sup>1</sup> ~~Details of certificate profiles forfor which the TLS/SSL certificate will be used. Subject Alternate Name(s) must be included. Details of certificate profiles for TLS/SSL~~ certificates may be found in the InCommon PKI repository as stated in Section 2.

Enhanced naming uses an extended organization field in an X.509v3 certificate to convey information through an organizational unit field. InCommon certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and any disclaimers of warranty that may apply. The lack of such information does not mean it does not apply to that certificate.

To communicate information InCommon may define:

- An organizational unit attribute.
- An InCommon standard resource qualifier to a certificate policy.
- Proprietary or other vendors' extensions.

### 3.1.2 Need for Names to be Meaningful

InCommon uses non-ambiguous designations and commonly used semantics to identify both the Issuer of the Certificate and the Subject of the Certificate.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

[Anonymity is not allowed. For pseudonymity, no specificationDoes not apply to SSL/TLS certificates.](#)

### 3.1.4 Rules for Interpreting Various name Forms

Distinguished Names in Certificates are X.501 compliant. For information on how X.501 Distinguished names are interpreted, please see RFC 2253 and RFC 2616.

---

<sup>1</sup> The Subject Name of a Certificate will at least contain a Country and Organization field, the exact contents for any Subscribing Institution will be determined at registration time.

### 3.1.5 Uniqueness of Names

Campuses should use Subject DNs that map uniquely to a single person/entity in perpetuity. However, if this is not possible, a campus must ensure that no two valid certificates containing the same Subject DN map to different persons/entities. While Subject DNs in expired or revoked certificates may map to different persons/entities than currently valid certificates, this practice should be avoided whenever possible. Multiple certificates with different Subject DNs may map to the same person/entity. The Distinguished Name in the Subject field of an InCommon CA issued Certificate is unique for each named Subject. Also, InCommon's CA assigns certificate serial numbers that appear in InCommon certificates. Assigned serial numbers are unique across all certificates issued by that CA.

The use of the SubjectAlt Email address and/or SubjectAlt/OtherName/PrincipalName is optional in InCommon certificates. However, if these fields are used, InCommon requires that these fields be populated with identifiers such that each field maps uniquely to the same single person/entity. Campuses must ensure that all SubjectAltName identifiers map to a single person/entity throughout the life of any valid certificate.

InCommon recommends the use of the email field in the Subject DN to guarantee uniqueness but a campus may use any appropriate mechanism to guarantee that the Subject DN uniquely maps to a single person/entity for the period of time that a certificate is valid. If an email address is used in the Subject DN, the email address must also be populated in the appropriate SubjectAltName field.

InCommon's CA assigns certificate serial numbers, which appear in InCommon certificates and which are unique across all certificates issued by that CA.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

InCommon does not permit the use of a name or symbol that infringes upon the intellectual property rights of another as stated in its subscriber agreements. However, InCommon does not verify or check the name appearing in a certificate for non-infringement. Subscribers are solely responsible for ensuring the legality of any information presented for use in an InCommon CA issued certificate. When submitting or approving a CSR, InCommon subscribers represent that they are not interfering with or infringing upon the rights of any third parties.

InCommon does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain's use of any infringing material. InCommon's CA may reject a CSR or revoke a certificate if it believes that any information in the certificate may be subject to infringement claims or ownership disputes.

## 3.2 Initial Identity Validation

InCommon validates the identity of Institutions that intend to issue end-user certificates. Institutions agree to only issue end-user certificates that indicate affiliation with the identified organization. InCommon or Comodo may refuse to issue an end-user certificate if it appears to be fraudulently issued. However it remains the Institution's responsibility to ensure that code signing certificates are issued to only appropriately identified parties each new Subscriber, its officially designated officers, and its domain names. For SSL/TLS certificates, InCommon validates only that the Subscriber has ownership of or administrative control for the Internet domain name(s) identified in its Subscriber Addendum or in later requests from Subscriber Registrars. Subsequently, subscriber Registrars are responsible to ensure the validity of any Subject information provided in a CSR. The InCommon CA will reject any CSR that includes a fully qualified domain name for which the Subscriber cannot be verified.

### 3.2.1 Method to Prove Possession of Private Key

Ownership of the private key is demonstrated through the submission of a valid CSR containing the matching public key.

### 3.2.2 Authentication of Organization Identity

InCommon may accept at its discretion any official organizational documentation supporting an application to become a Subscriber. InCommon may also use the services of a third party to validate and confirm information. Sources include

- official organizational documentation, such as business licenses, articles of incorporation, sales license or other relevant documents.
- Third-party services or records such as bank statements, records of accreditation status, or other relevant documents.

Verification can occur through an automated process or a manual review.

InCommon also verifies the identity of Subscriber's designated officers – an official executive and Subscriber Registrars designated by the executive – using out-of-band means to verify contact information and to make contact with each officer for credentialing and Subscriber Registrar's subsequent authentication to the certificate management UI.

### 3.2.3 Authentication of Individual Identity

Code Signing Certificates may be issued to individuals or to specifically identified departmental or laboratory organizations. An institution may also elect to have a single code signing certificate or a group of certificates that identify the organization at large.~~Not applicable to SSL/TLS certificates.~~

It is the responsibility of subscriber institutions to authenticate and identify individual entities for which it will be issuing code signing certificates.

Subscriber institutions will issue certificates to its end users and/or specifically identified departmental organizations using a process that is at least as strong as its existing practice for managing accounts for central services such as electronic mail, calendaring, and access to central file storage.

#### 3.2.3.1 Special Rule for Code Signing Certificates

Code Signing certificates are used by software on relying party's computers to verify that software downloaded and intended to run on their computer in fact originates from the source named in the certificate. However most software verification systems ONLY DISPLAY THE COMMON NAME FIELD of the code signing certificate used. It is therefore the responsibility of the Subscriber to ensure that this field properly identifies the entity responsible for the software. This field SHOULD NOT be filled in so as to confuse the relying party as to the origin of the software or otherwise represent itself in a fraudulent manner.

### 3.2.4 Non-Verified Subscriber Information

InCommon verifies only the information listed as validated in section 4.2. Any other information provided by Subscriber Registrars is not verified by InCommon.

### 3.2.5 Validation of Authority

The authority of a Subscriber to be issued a certificate is first confirmed as described in section 3.2.2. Subscribers must notify InCommon if any Subscriber Registrar misrepresents his or her affiliation with or authority regarding Subscriber and Subscriber's affiliated end user with a WHOIS check or by a practical demonstration of the Subscriber Registrar's authority to act on behalf of the domain owner. Subscribers must notify InCommon if any Subscriber Registrar misrepresents his or her affiliation with or authority regarding Subscriber and Subscriber's domains.

### 3.2.6 Criteria for Interoperation

No stipulation.

## 3.3 Identification and Authentication for Re-key Requests

### 3.3.1 Identification and Authentication for Routine Re-key

It is the responsibility of Subscriber institutions to determine policies related to routine re-keying.~~Any Registrar or Requester can request a re-key by submitting an appropriate CSR.~~

### 3.3.2 Identification and Authentication for Re-key After Revocation

Subscriber institutions determine the mechanism for authenticating end-users prior to issuing certificates including after the revocation of a certificate.~~Not applicable to InCommon SSL/TLS certificates.~~

### 3.4 Identification and Authentication for Revocation Request

It is the responsibility of Subscriber institutions to authenticate user certificate revocation requests. Authorized staff at subscriber institutions will have access to appropriate software/websites to effect revocation as necessary for code signing certificates issued to end-entities of their institution. Self-revocation by individual certificate holders will be allowed on a case by case basis, per Subscriber institution's preference. Prior to revoking a certificate, the InCommon CA verifies that the revocation was requested by the certificate Requester or an authorized Registrar associated with the Subscriber. InCommon may, if necessary, also request that the revocation request be made by the Subscriber's Executive contact. Upon receipt of an unconfirmed revocation request, the InCommon CA may request out-of-band confirmation from a known Subscriber Registrar or Executive.

## 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 Certificate Application

Code Signing certificates are issued either via a website operated by Comodo or via a website operated by Subscriber which interacts with an Application Programming Interface (API) provided by Comodo. End-users submit their CSRs to this website and authorized Subscriber Registrars from the Subscriber institution or an automated process approve the request prior to the issuance of the certificate. Alternatively certificates are issued by a programming API. In this case credentials to access this API are issued to approved contacts at the subscribing institution. The institution then runs a system of its own design to authenticate certificate requests and forward them to Comodo for issuance, using the API and provided credentials.

InCommon certificates are issued to authorized organizations and individuals who submit a certificate signing request and successfully complete the required validation procedures described herein. Prior to the issuance of a certificate, the InCommon CA will validate a request in accordance with this CPS. Validation of the request will involve the information provided by the Subscriber upon completion of their subscription contract and verified by InCommon prior to accepting the certificate request.

#### Who Can Submit a Certificate Application

Any person affiliated with a subscribing institution may apply for a certificate. It is the responsibility of the subscribing institution to determine whether or not issuing a certificate is appropriate.

SSL/TLS certificate requests may be submitted by an authorized Registrar or an authorized Subscriber Requester

#### Enrollment Process and Responsibilities

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 4.2 Certificate Application Processing

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 4.2.1 Performing Identification and Authentication Functions

The Comodo website or API server validates that the "Country", "Domain Name" and "Organization" fields of submitted CSRs are correct as determined at subscription time. It is the responsibility of the Subscriber institution to ensure that other relative distinguished name components are accurate for a given code signing certificate. In particular the institution must ensure that the Common Name (CN) relative distinguished name is properly provided. See 3.2.3.1 InCommon Registration Authority validates the following required information in any SSL/TLS certificate. Other optional certificate subject information is considered under the purview of Subscriber Registrars and is detailed in the certificate profile found in the InCommon Repository.

- O (Organization): Legal Name of the Organization or a commonly understood and unique variant of Legal Name

- ~~Common Name (CN): Fully Qualified Domain Name or Network Server Name or Public or Private Host Name~~
- Approval or Rejection of Certificate Applications

~~Subscriber Registrars are responsible for the approval of individual CSRs and/or for the correct operation of software that validates CSR submissions on behalf of end-users. Both InCommon and Comodo may reject the issuance of a certificate if there are reasons to believe that appropriate end-user authentication is not being properly performed, the sub-domains represented in CSRs, and generally for the management of Subscriber certificates beyond the approvals of the Master Registrar stated in section 4.2.1.~~

#### 4.2.2 Time to Process Certificate Applications

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 4.3 Certificate Issuance

InCommon may refuse to issue a certificate to any party as InCommon sees fit. InCommon is not obligated to disclose the reasons for such a refusal.

#### 4.3.1 CA Actions During Certificate Issuance

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

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

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 4.4 Certificate Acceptance

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

#### 4.4.2 Publication of the Certificate by the CA

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

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

No stipulation.

### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

~~Certificates and associated private keys may only be used for lawful and appropriate purposes as set forth in this CPS. Subscribers and their end users are responsible for protecting their private keys from unauthorized use of the Private Key in conjunction with a certificate issued by this CA is prohibited until the Subscriber has agreed to a Subscriber agreement. Certificates may only be used for lawful and appropriate purposes as set forth in this CPS. Subscribers are responsible for protecting their private keys from unauthorized use and agree to immediately cease using the private key in conjunction with a Certificate following the expiration or revocation of the Certificate.~~

#### 4.5.2 Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party.

### 4.6 Certificate Renewal

Renewal request requirements and procedures are treated as new certificate requests.

#### 4.6.1 Circumstance for Certificate Renewal

n/a.

#### 4.6.2 Who May Request Renewal

n/a.

#### 4.6.3 Processing Certificate Renewal Requests

n/a.

#### 4.6.4 Notification of New Certificate Issuance to Subscriber

n/a.

#### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

n/a.

#### 4.6.6 Publication of the Renewal Certificate by the CA

n/a.

#### 4.6.7 Notification of Certificate Issuance by the CA to other Entities

n/a.

### 4.7 Certificate Re-key

~~Certificate rekey is the issuance of a new certificate that certifies a new public key for the same Subject.~~ Rekey request requirements and procedures are treated as new certificate requests.

#### 4.7.1 Circumstance for Certificate Re-Key

n/a.

#### 4.7.2 Who May Request Certification of a New Public Key

n/a.

#### 4.7.3 Processing Certificate Re-keying Requests

n/a.

#### 4.7.4 Notification of New Certificate Issuance to Subscriber

n/a.

#### 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

n/a.

#### 4.7.6 Publication of the Re-keyed Certificate by the CA

n/a.

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

n/a.

### 4.8 Certificate Modification

~~Certificate information may change during the life of the certificate. It is the responsibility of subscriber institutions to ensure new certificates are issued as appropriate. In this case, the InCommon CA will issue a new certificate based on the new information rather than modifying an existing certificate.~~ Modification request requirements and procedures are treated as new certificate requests

#### 4.8.1 Circumstance for Certificate Modification

n/a.

#### 4.8.2 Who May Request Certificate Modification

n/a.

#### 4.8.3 Processing Certificate Modification Requests

n/a.

#### 4.8.4 Notification of New Certificate Issuance to Subscriber

n/a.

#### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

n/a.

#### 4.8.6 Publication of the Modified Certificate by the CA

n/a.

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

n/a.

### 4.9 Certificate Revocation and Suspension

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the CRL and OCSP server and will remain available in those locations until some time after the end of the certificate's validity period.

InCommon does not make use of certificate suspension.

#### 4.9.1 Circumstances for Revocation

Revocation of a certificate is the permanent end of the operational period of the certificate prior to reaching the conclusion of its stated validity period. It is the Subscriber's responsibility to revoke any certificate whose private key becomes compromised or for any of the other conditions described in the Subscriber Addendum. Comodo or InCommon may revoke a digital certificate under any of the conditions described in the Subscriber Addendum.

#### 4.9.2 Who can Request Revocation

The Subscriber, the Requester, or other appropriately authorized parties can request revocation of a certificate.

#### 4.9.3 Procedure for Revocation Request

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 4.9.4 Revocation Request Grace Period

There is no revocation grace period.

#### 4.9.5 Time Within Which CA Must Process the Revocation Request

The processing time is dependent upon the Subscriber Registrar's ability to respond appropriately in his or her role as Subscriber's certificate lifecycle manager. System response time is provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must always check the status of the Certificate on which they are relying. Relying Parties may check the OCSP and/or CRL to confirm that the certificate has not been revoked.

#### 4.9.7 CRL Issuance Frequency (if applicable)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. Typically an updated CRL is published every 24 hours and remains valid for 5 days. Under special circumstances the CRL may be published more frequently.

#### 4.9.8 Maximum Latency for CRLs (if applicable)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 4.9.9 On-line Revocation and Status Checking Availability

The InCommon CA manages and makes publicly available information about revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by the InCommon CA are X.509v2 CRLs as profiled in RFC4630. Users and relying parties are strongly urged to check the status of certificates at all times prior to relying on information featured in a certificate. The CRL and OCSP locations are available in the InCommon Server Certificate Profile found in the InCommon Repository.

#### 4.9.10 On-line Revocation Checking Requirements

Relying Parties must confirm the validity of a certificate via the CRL or OCSP mechanisms prior to relying on the Certificate.

#### 4.9.11 Other Forms of Revocation Advertisements available

n/a.

#### 4.9.12 Special Requirements Re-key Compromise

No stipulation.

#### 4.9.13 Circumstances for Suspension

The InCommon CA does not utilize certificate suspension.

#### 4.9.14 Who can Request Suspension

n/a.

#### 4.9.15 Procedure for Suspension Request

n/a.

#### 4.9.16 Limits on Suspension Period

n/a.

### 4.10 Certificate Status Services

#### 4.10.1 Operational Characteristics

Each CRL and the OCSP server contains information for all of InCommon's revoked certificates until they expire.

All expired CRLs are archived as described and Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

Individual entries into the OCSP can be requested using the InCommon OCSP server. Revoked certificates are identified in the OCSP immediately after their revocation.

#### 4.10.2 Service Availability

The OCSP server provides access to certificate status information 24x7. CRLs are open to public inspection 24x7. This is non-inclusive of scheduled maintenance and SLA downtime allowances of 99.9% availability.

### 4.10.3 Optional Features

n/a.

### 4.11 End of Subscription

Withdrawal and termination are described in the Subscriber Addendum.

### 4.12 Key Escrow and Recovery

The InCommon CA escrows Subscriber private keys only upon the Subscriber institution's request. Escrowed keys are kept in encrypted databases provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. If a Subscriber recovers an escrowed private key, the corresponding certificate is automatically revoked~~does not escrow Subscriber private keys.~~

## 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

### 5.1 Physical Controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.1 Site Location and Construction

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.2 Physical Access

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.3 Power and Air Conditioning

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.4 Water Exposures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.5 Fire Prevention and Protection

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.6 Media Storage

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.7 Waste Disposal

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.1.8 Off-site Backup

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.2 Procedural Controls

#### 5.2.1 Trusted Roles

Trusted roles for InCommon are defined as the RA personnel who verify the Subscriber organization status and the identity proofing of Subscriber Registrars and the assignment of Subscriber Registrar credentials to the management interface. InCommon RA personnel are also responsible for the approval process of all Subscriber information as described in section 4.2 above-submitted fully-qualified domain names.

Trusted roles for the physical operation of the CA and certificate request and revocation servers are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 5.2.2 Number of Persons Required Per Task

InCommon requires one RA for organizational vetting ~~and identity proofing and two RA personnel for the approval of all host names.~~

For the physical operation of the CA, requirements are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 5.2.3 Identification and Authentication for Each Role

All InCommon personnel present at least two forms of identification to its human resources department to ensure accurate identification.

For the physical operation of the CA, requirements are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 5.2.4 Roles Requiring Separation of Duties

RA and physical CA operations roles are separated between InCommon and Comodo.

For the physical operation of the CA, requirements are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 5.3 Personnel Controls

### 5.3.1 Qualifications, Experience, and Clearance Requirements

InCommon follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. All InCommon trusted personnel must have the necessary qualifications, experience, or training to fulfill their job descriptions.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

### 5.3.2 Background Check Procedures

Background checks are performed on all trusted InCommon personnel before access is granted to InCommon's systems. These checks include, but are not limited to, criminal history and employment history (for references).

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

### 5.3.3 Training Requirements

Personnel training occurs via a mentoring process involving senior members of the team to which the employee is attached. The training program is periodically reviewed and enhanced as necessary.

Training programs are tailored toward each individual's job responsibilities and include training on PKI concepts, job responsibilities, operational policies and procedures, incident handling and reporting, and disaster recovery procedures.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

### 5.3.4 Retraining Frequency and Requirements

Personnel are required to attend refresher training courses to ensure that they can competently and satisfactorily perform their job responsibilities.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

### 5.3.5 Job Rotation Frequency and Sequence

No Stipulation

### 5.3.6 Sanctions for Unauthorized Actions

Personnel violating a policy or procedure are subject to disciplinary action. The action taken depends on the circumstances surrounding the action, the severity of the violation, and the personnel's past performance. In some cases, disciplinary action may include the personnel's termination.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

### 5.3.7 Independent Contractor Requirements

If an independent contractor or consultant is used, InCommon will first ensure that each such contractor or consultant is first obligated to abide by the same functional and security criteria that are set forth herein. Contractors and consultants are subject to the same sanctions as other personnel as set forth in Section [5.3.65-3-6](#).

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

### 5.3.8 Documentation Supplied to Personnel

No stipulation.

## 5.4 Audit Logging Procedures

### 5.4.1 Types of Events Recorded

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.2 Frequency of Processing Log

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.3 Retention Period for Audit Log

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.4 Protection of Audit Log

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.5 Audit Log Backup Procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.6 Audit Collection System (internal vs. external)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.7 Notification to Event-Causing Subject

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.4.8 Vulnerability Assessments

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 5.5 Records archival

### 5.5.1 Types of records archived

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.5.2 Retention period for archive

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.5.3 Protection of archive

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.5.4 Archive backup procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.5.5 Requirements for time-stamping of records

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.5.6 Archive collection system

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.5.7 Procedures to obtain and verify archive information

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.6 Key changeover

Towards the end of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in section [6.16.4](#) of this CPS.

### 5.7 Compromise and disaster recovery

#### 5.7.1 Incident and compromise handling procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.7.2 Computing resources, software, and/or data are corrupted

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.7.3 Entity Private Key Compromise Procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

#### 5.7.4 Business continuity capabilities after a disaster

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 5.8 CA or RA termination

If Internet2 must cease operation, Internet2 will make a commercially reasonable effort to notify all participants in advance of the effective date of the termination as described in the Subscriber Addendum.

## 6 TECHNICAL SECURITY CONTROLS

The Comodo sites hosting InCommon's PKI CA are under a security policy designed to detect, deter and prevent unauthorized logical or physical access to CA related facilities. This is provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.1 Key pair generation and installation

#### 6.1.1 Key pair generation

InCommon CA's private keys are securely generated and protected by Comodo as part of the Comodo Agreement. The InCommon [code signing CA can generate key pairs for end-user certificates and, when it does, distribute the private keys to individuals through a secure channel provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. A Subscriber institution can also upload CSRs, creating its own key pair](#)~~CA does not generate key pairs for end-entity certificates.~~

#### 6.1.2 Private key delivery to subscriber

[If keys are generated by the Comodo-hosted system \(for example, through the web-based self-enrollment system\), key delivery specifications are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.](#)~~Not applicable.~~

### 6.1.3 Public key delivery to certificate issuer

Certificate requests are generated using Subscriber's software, and the request is submitted to the InCommon CA's approval workflow in the form of a PKCS #10 Certificate Signing Request (CSR).

### 6.1.4 CA public key delivery to relying parties

InCommon delivers issued certificates to certificate requesters. InCommon PKI root certificates are provided by Comodo, which protects the root CAs that issue the InCommon CA certificates.

The AddTrust External CA Root certificate is present in commonly available web browsers and other device stores and is made available to relying parties through these methods.

### 6.1.5 Key sizes

Key pairs are of sufficient length to prevent unauthorized determination or reverse engineering of the private key. InCommon's Intermediate CA keys sizes are 2048 bit. For [code signing certificates](#), ~~InCommon strongly recommends 2048 bit keys. its server certificates, InCommon strongly recommends 2048 bit keys and sets this as the default. Server certificates of 1024 bit key sizes will be accepted. This is also reflected in the Server certificate profile found in the Repository.~~

### 6.1.6 Public key parameters generation and quality checking

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The key usage field extension in InCommon Certificates specifies the purpose for which the Certificate and key pair may be used. Enforcement of the limitations of use found in this field is beyond InCommon's control as correct use is highly dependent on having the correct software.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

Protection of InCommon CA key pairs is provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.1 Cryptographic module standards and controls

Comodo CA Limited protects CA cryptographic key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliance are available at its official website ([www.comodogroup.com](http://www.comodogroup.com)).

### 6.2.2 Private key (n out of m) multi-person control

For InCommon CA key recovery purposes, the InCommon CA signing keys will be encrypted and stored within a secure environment. InCommon's escrowed copy of the private key is split across a number of removable media and requires a subset of the number to reconstruct. Custodians in the form of two or more InCommon authorized officers are required to physically retrieve the removable media from the distributed physically secure locations.

### 6.2.3 Private key escrow

~~Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. InCommon does not escrow end-entity private keys.~~

### 6.2.4 Private key backup

InCommon's CA keys are generated and stored by Comodo as part of the Comodo Agreement.

~~Subscribers and their end users are solely responsible for protection of their private keys. InCommon maintains no involvement in the protection of such keys. re solely responsible for protection of their private keys. InCommon maintains no involvement in the generation, protection or distribution of such keys. InCommon strongly urges Subscribers to use a password or stronger authentication method to prevent unauthorized access and usage of the Subscriber private key.~~

### 6.2.5 Private key archival

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.6 Private key transfer into or from a cryptographic module

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.7 Private key storage on cryptographic module

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.8 Method of activating private key

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.9 Method of deactivating private key

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.10 Method of destroying private key

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.2.11 Cryptographic Module Rating

See Section [6.2.16-2.1](#).

## 6.3 Other aspects of key pair management

No stipulation.

### 6.3.1 Public key archival

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.3.2 Certificate operational periods and key pair usage periods

The operational period of each Certificate generated ends upon its revocation or expiration. The validity period of InCommon certificates varies dependent on the certificate type, but typically, a certificate will be valid for 1 to 3 years. InCommon reserves the right to, at its discretion, issue certificates that may fall outside of these set periods.

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.4.2 Activation data protection

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.4.3 Other aspects of activation data

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 6.5 Computer security controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.5.1 Specific computer security technical requirements

InCommon computer systems are set up and maintained in a secure manner that prevents unauthorized access. The InCommon CA computers are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 6.5.2 Computer security rating

No Stipulation.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.6.2 Security management controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 6.6.3 Life cycle security controls

No Stipulation.

## 6.7 Network security controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 6.8 Time-stamping

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 7 CERTIFICATE, CRL, AND OCSP PROFILES

This CPS covers only [code signingSSL/TLS-Server](#) certificates.

InCommon may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of InCommon products creates no claims by any third party. If necessary, InCommon will amend this CPS or create a separate CPS upon the inclusion of a new certificate product in the InCommon hierarchy. The CPS will usually be made public on the official InCommon websites at least seven (7) days prior to the offering such new product.

Revoked certificates are appropriately referenced in the CRL and/or OCSP.

### 7.1 Certificate profile

In order to use and rely on an InCommon certificate, the relying party must use X.509v3 compliant software. Supported certificate profiles are listed in the InCommon Repository.

#### 7.1.1 Version number(s)

See the [code signingSSL/TSL-server](#) certificate profile in the InCommon Repository.

#### 7.1.2 Certificate extensions

The InCommon CA uses the standard X.509, version 3, to construct digital certificates for use within the InCommon PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. InCommon uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

#### 7.1.3 Algorithm object identifiers

Refer to the Certificate Profile found in the repository.

#### 7.1.4 Name forms

Refer to the Certificate Profile found in the repository.

#### 7.1.5 Name constraints

No Stipulation.

### 7.1.6 Certificate policy object identifier

A Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy or a certification practices statement (CPS).

Specific InCommon certificate profiles are found in the InCommon Repository, and any relevant OIDs are provided in Appendix B.

### 7.1.7 Usage of Policy Constraints extension

No Stipulation

### 7.1.8 Policy qualifiers syntax and semantics

The InCommon CA includes information in the Policy Qualifier field of the Certificate Policy extension that puts Relying Parties on notice as to the location of its CPS. This field usually includes a URL that points the Relying Party to the Relying Party Agreement, the CPS, and other documents in the repository where they can find out more about the limitations on liability and other terms and conditions governing the use of the Certificate.

### 7.1.9 Processing semantics for the critical Certificate Policies extension

No Stipulation.

## 7.2 CRL profile

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 7.2.1 Version number(s)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 7.2.2 CRL and CRL entry extensions

No Stipulation.

## 7.3 OCSP profile

OCSP is a way for users to obtain information about the revocation status of an InCommon CA issued Certificate. The InCommon CA uses OCSP to provide information about any of its revoked certificates that are unexpired. OCSP responders conform to RFC 2560.

### 7.3.1 Version Number(s)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

### 7.3.2 OCSP Extensions

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

### 8.1 Frequency or Circumstances of Assessment

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 8.2 Identity/Qualifications of Assessor

Provided by Comodo as stated in the Comodo CPS.

## 8.3 Assessor's Relationship to Assessed Entity

Provided by Comodo as stated in the Comodo CPS.

## 8.4 Topics Covered by Assessment

Provided by Comodo as stated in the Comodo CPS.

## 8.5 Actions Taken as a Result of Deficiency

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

## 8.6 Communication of Results

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

# 9 OTHER BUSINESS AND LEGAL MATTERS

While the structure of this CPS has been left intact as a matter of RFC form, the representations, warranties and limitations associated with this service are described in detail and governed by the provisions in the InCommon Participation Agreement and the Certificate Service Addendum.

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

Fees are detailed on the official InCommon website ([www.incommon.org/cert](http://www.incommon.org/cert)). InCommon may change these fees pursuant to its rights under the Subscriber Addendum.

### 9.1.2 Certificate Access Fees

Currently, InCommon does not charge a fee for Certificate access but may in the future. Charges may be incurred for extensive or time-consuming searches. Fees for such extensive use are negotiated on an individual basis.

### 9.1.3 Revocation or Status Information Access Fees

InCommon does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of an InCommon-issued certificate using its CRLs or OCSP.

### 9.1.4 Fees for Other Services

Fees for other services offered by InCommon are set either within the individual agreements with the parties or are detailed on the official InCommon website, depending on the services required.

### 9.1.5 Refund Policy

Subscriber refunds are described in the Subscriber Addendum.

## 9.2 Financial Responsibility

InCommon accepts no financial responsibility.

### 9.2.1 Insurance Coverage

Refer to the Subscriber Addendum and Relying Party Agreement.

### 9.2.2 Other Assets

InCommon accepts no financial responsibility

### 9.2.3 Insurance or Warranty Coverage for End-Entities

InCommon provides no warranty as further described in the Subscriber Addendum and Relying Party Agreement.

## 9.3 Confidentiality of Business Information

InCommon observes the following rules on the protection of business information:

### 9.3.1 Scope of Confidential Information

InCommon keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Executed Subscriber agreements when not in violation with applicable state, federal, or other law (for example, state "sunshine" laws).
- Financial transaction records and financial audit records.
- External or internal audit trail records and reports.
- Certain portions of its contingency plans and disaster recovery plans.
- Internal tracking and records on the operations of the PKI infrastructure, certificate management and enrollment services and data.
- ~~Subscriber Registrar email address and telephone if requested by Subscriber Registrar~~  
~~Proof of existence and organizational status of the Organization if marked Confidential by Subscriber~~
- ~~Proof of existence and organizational status of the Organization if marked Confidential by Subscriber~~
- Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all certificates issued by the InCommon CA is public information. Subscriber data marked as "Public" or submitted as part of a certificate request is not confidential and is published within an issued digital certificate in accordance with this CPS.

### 9.3.2 Responsibility to Protect Confidential Information

All personnel in trusted positions handle all confidential information in strict confidence. InCommon is not required to and does not release any confidential information, unless otherwise required by law or by obtaining consent from the party to whom the confidential information belongs, without an authenticated, reasonably specific request by an authorized party specifying:

- The consent of the party to whom InCommon owes a duty to keep information confidential.
- The name of the party requesting such information.
- A court order, if any.

## 9.4 Privacy of Personal Information

### 9.4.1 Privacy Plan

InCommon has implemented a privacy policy, which complies with this CPS. The InCommon privacy policy is published in the InCommon repository described in section 2.

### 9.4.2 Information Treated as Private

Any information about the designated officers of Subscriber organizations that is not publicly accessible or available through the content of the issued certificate, a CRL, or the OCSP is treated as private information. Subscriber organizations are responsible for the personal information of their delegated officers and constituents.

### 9.4.3 Information Not Deemed Private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered private. Information about Subscribers available in public directories or databases is also not considered private.

### 9.4.4 Responsibility to Protect Private Information

All InCommon personnel receiving private information are responsible for protecting such information from compromise and disclosure to third parties. Each party will use the same degree of care that it exercises with respect to its own information of like importance, but in no event will the degree of care be less than a reasonable degree of care.

### 9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, the applicable privacy policy, or by agreement, InCommon will use private information only for its own business purposes related to the services it provides to Subscriber and will not share that information with external parties except as required for by law or with the permission of the subject.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

InCommon is entitled to disclose any confidential or private information, if InCommon believes, in good faith, that the disclosure is necessary in response to subpoenas and search warrants or if disclosure is necessary in response to a pending legal proceeding or a state's mandated sunshine laws.

### 9.4.7 Other Information Disclosure Circumstances

No Stipulation.

## 9.5 Intellectual Property Rights

InCommon or its partners or associates own all intellectual property rights associated with its databases, websites, InCommon digital certificates and any other publication originating from InCommon, including this CPS.

### 9.5.1 Certificates

Certificates are the property of InCommon. InCommon gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. InCommon reserves the right to revoke the certificate pursuant to revocation terms in the Subscriber Addendum. Private and public keys are the property of the subscriber's Subjects who rightfully generate and hold them.

Subscribers represent that their use of the certificate does not interfere with or infringe on any rights of third parties. The Subscriber represents that it is not seeking to use the issued certificate's domain and distinguished names for any unlawful purpose, including tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

### 9.5.2 Copyright

Copyright © 2011<sup>10</sup> by Internet2. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for commercial advantage and that copies bear this notice. Abstracting or creation of derivative works with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission.

### 9.5.3 Trademarks

See Subscriber Addendum.

#### 9.5.4 Infringement

InCommon does not provide infringement resolution services. Subscribers are responsible for their own use of certificates. See the Subscriber Addendum for legal protections, rights and responsibilities.

### 9.6 Representations and Warranties

Subscribers, Subjects, relying parties and any other parties must not interfere with or reverse engineer the technical implementation of InCommon PKI services, including, but not limited to, the key generation process, the public website, and the InCommon repositories except as explicitly permitted by this CPS or upon prior written approval of InCommon or Comodo as appropriate. Results of failure to comply with this as a subscriber is described in the Subscriber Addendum. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the InCommon repository and any Digital Certificate or Service provided by InCommon.

All parties – subscribers, certificate subjects, relying parties, and any others – are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as in using PKI as a solution to their security requirements.

#### 9.6.1 CA Representations and Warranties

Other than the representations and warranties already detailed in this CPS, see Subscriber Addendum and InCommon Participation Agreement.

#### 9.6.2 RA Representations and Warranties

Other than the representations and warranties already detailed in this CPS, see Subscriber Addendum and InCommon Participation Agreement.

#### 9.6.3 Subscriber Representations and Warranties

Other than the representations and warranties already detailed in this CPS, see Subscriber Addendum and InCommon Participation Agreement

#### 9.6.4 Relying Party Representations and Warranties

See the Relying Party Agreement in the InCommon Repository.

#### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

### 9.7 Disclaimers of Warranties

InCommon disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose. See the Subscriber Addendum and InCommon Participation Agreement (found in the InCommon Repository) for further information.

### 9.8 Limitations of Liability

See the Subscriber Addendum and InCommon Participation Agreement (found in the InCommon Repository) for further information.

### 9.9 Indemnities

#### 9.9.1 Subscriber Indemnity to InCommon

Indemnification by Subscriber to InCommon, if any, is described in the InCommon Subscriber Addendum.

#### 9.9.2 Subscriber Indemnity to Relying Parties

No stipulation.

## 9.10 Term and Termination

### 9.10.1 Term

This CPS and any amendments are effective seven days after being published to the Repository and remain effective until replaced with a newer version.

### 9.10.2 Termination

In case of termination of CA operations for any reason whatsoever except in the case of force majeure, InCommon will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Details are provided in the Subscriber Addendum, available in the repository.

### 9.10.3 Effect of Termination and Survival

Details are provided in the Subscriber Addendum, available in the repository.

## 9.11 Individual notices and Communications with Participants

InCommon accepts notices related to this CPS by means of email messages or in paper form to the InCommon point of contact listed in section 1.5.2. For communication issues related to the performance of certificates or the designation of Subscriber Executives and Registrars, secure communication will be required, either through out-of-band means such as telephone, through authorized web-based transactions or email secured by digital signature.

## 9.12 Amendments

The InCommon PA is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition. Amendments to this CPS may be made from time to time as approved by the InCommon PA and Comodo. Amendments may be in the form of either an amended form of the CPS or made available as a supplemental document in InCommon's repository.

### 9.12.1 Procedure for Amendment

Updates supersede any designated or conflicting provisions of the referenced version of the CPS and are indicated through appropriate revision numbers and publication dates. Revisions that are not deemed significant by InCommon (those amendments or additions that have minimal or no impact on Subscribers or Relying Parties), are made without notice and without changing the version number of this CPS.

### 9.12.2 Notification Mechanism and Period

Upon the PA approving such changes deemed to have significant impact on the users of this CPS, an updated edition of the CPS will be published in the InCommon repository, with seven (7) days notice given to Subscribers via email of upcoming changes. Suitable incremental version numbering will identify new editions.

### 9.12.3 Circumstances Under Which OID Must be Changed

If InCommon decides that a material change in InCommon's certificate policy warrants a change in the currently specified OID for a particular certificate type, then the revised CPS or amendment thereto will contain a revised OID for that type of certificate.

## 9.13 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution, a party must notify InCommon of the dispute with a view to seek a resolution. Parties must work with InCommon in good faith to resolve issues in a reasonable manner prior to third party involvement.

## 9.14 Governing Law

Details are provided in the InCommon Certificate Service Subscriber Addendum, available in the repository. This choice of law is made to provide uniform interpretation of this CPS, regardless of the place of residence or place of use of InCommon's certificates.

## 9.15 Compliance with Applicable Law

All parties agree to abide by all applicable laws when validating, issuing, or using certificates.

## 9.16 Miscellaneous Provisions

### 9.16.1 Entire Agreement

This CPS is not the entire agreement between any parties. All parties must accept additional agreements prior to receiving, using, or relying on a digital certificate. Section headings are for reference and convenience only and are not part of the interpretation of the CPS.

### 9.16.2 Assignment

This CPS is binding upon all successors and representatives of any party. The rights in this CPS are assignable.

### 9.16.3 Severability

Any provision held invalid or unenforceable will be reformed to the minimum extent necessary to make the provision valid and enforceable. If reformation is not possible, the provision is deemed omitted and the balance of the CPS remains valid and enforceable.

### 9.16.4 Enforcement

InCommon's failure to enforce any provision of this CPS does not waive its right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, all waivers must be both in writing and signed by InCommon. Agreements between InCommon and various parties control in the event of a conflict between this CPS and the Subscriber Addendum.

Except where an express time frame is set forth in this CPS, any delay or omission by any party will not impair or be construed as a waiver of such right, remedy or power.

### 9.16.5 Force Majeure

InCommon is not liable for a delay or failure to perform an obligation to the extent that the delay or failure is caused by an occurrence beyond the party's reasonable control. The operation of the Internet is beyond InCommon's reasonable control, and InCommon is not responsible for a delay or failure caused by an interruption or failure of telecommunication or digital transmission links, Internet slow-downs or failures, or other such transmission failure.

## 9.17 Other Provisions

No Stipulation

## Acknowledgments

The InCommon Policy Authority acknowledges the considerable efforts of the research and education community in the development of this CPS. Specifically a task force under the InCommon Technical Advisory Committee, a PKI advisory committee, edited and contributed to this document: Jim Jokl (Chair), University of Virginia; Jim Basney, National Center for Supercomputing Applications; Paul Caskey, University of Texas System; Michael Gettes, [Carnegie Mellon University](#); [Garick Hamlin, University of Pennsylvania](#); [Dan Jones, University of Colorado](#); [John Krienke, InCommon/Internet2](#); [David Walker, University of California, Davis](#); [David Wasley, ret., University of California Office of the President](#); and [Jeffrey I. Schiller, Massachusetts Institute of Technology/MIT](#); [Garick Hamlin, University of Pennsylvania](#); [Dan Jones, University of Colorado](#); [John Krienke, InCommon/Internet2](#); [Scott Rea, Dartmouth University](#); [David Walker, University of California, Davis](#); and [David Wasley, ret., University of California Office of the President](#).

APPENDIX A

**PKI HIERARCHY**

Comodo AddTrust External CA: UTN-USERFirst-Object: InCommon Code Signing CA: Subscriber Code-SigningInCommon Intermediate SSL CA: Subscriber Server Certificates

APPENDIX B

**CERTIFICATE OBJECT IDENTIFIERS**

CPS OID 1.3.6.1.4.1.5923.1.4.3.21.1