

# **Certificate Practice Statement (CPS)**

## **Colby College Certificate Authority**

### **Contents**

- 1.0 Introduction
  - 1.1 Identification
  - 1.2 Repositories
  - 1.3 Sponsors
  - 1.4 Contacts
- 2.0 General Provisions
  - 2.1 Subscriber Obligations
  - 2.2 Publication and Repository
- 3.0 Identification and Authentication
  - 3.1 Need for Names to be Meaningful
  - 3.2 Method to Prove Possession of Private Key
  - 3.3 Authentication of Individual Entity
  - 3.4 Authentication for Routine Renewal of Certificates
  - 3.5 Authentication of Revocation Request
- 4.0 Operational Requirements
  - 4.1 Application for a Certificate
  - 4.2 Certificate Revocation
    - 4.2.1 Circumstances for Revocation
    - 4.2.2 Revocation Request Grace Period
    - 4.2.3 Entity Public Certificate is Revoked
    - 4.2.4 CSS Publishing Frequency
  - 4.3 Recorded Events
    - 4.3.1 Frequency of Processing Audit Logs
  - 4.4 Records Archival
  - 4.5 Secure Facility after a Natural or Other Type Disaster
- 5.0 Physical, Procedural and Personnel Security
  - 5.1 Site Location, Construction and Physical Access
  - 5.2 Trusted roles
  - 5.3 Number of Person Required per Task
  - 5.4 Background, Qualifications, Experience, and Clearance Requirements
- 6.0 Technical Security Controls
  - 6.1 CA Private Signing Key
  - 6.2 Network Security Controls
  - 6.3 Life-Cycle Security Assurance

### Appendices

- Appendix A: CA Personnel
- Appendix B: Subscriber Agreement

Certificate Practice Statement for Colby College CA

**Revision History**

<b>Version</b>	<b>Date</b>	<b>Comment</b>
0.1	2007-06-07	Initial Version
0.2	2008-04-10	Draft version for CA working group review
0.3	2008-04-17	Draft version for CA working group review
0.4	2008-05-02	Draft version for CA working group review
0.5	2008-05-13	Draft version for ITS-ISDS group review
1.0	2008-08-05	First version for general release

## **1.0 Introduction**

This is the Certificate Practice Statement (CPS) for the Colby College certificate authority (CA). It states the practices the CA employs in issuing and managing digital certificates. This CPS outlines the technical, procedural and personnel policies and practices of Colby College with regard to the management and operation of its public key infrastructure (PKI) and CA.

### **1.1 Identification**

The CPS has been reviewed and approved by the Colby College Information Technology Services (ITS) department and the Information Systems and Data Security (ISDS) working group.

This CPS document is published at URL: <http://www.colby.edu/CPS>

### **1.2 Repositories**

See section 2.6

### **1.3 Sponsors**

The sponsor of the Colby College CA is Colby College. The sponsor of a Colby College signed certificate is the prefect of the department in Colby College that issued the certificate signing request.

### **1.4 Contacts**

This policy is administered by the CA administrators of the Colby College ITS department:

Colby College ITS / CA Administrators  
4200 Mayflower Hill Drive  
Waterville, ME 04901  
United States of America

Or, via Email: [rootca@colby.edu](mailto:rootca@colby.edu)

Further information can be found at <http://www.colby.edu/CPS>

## **2.0 General Provisions**

### **2.1 Subscriber Obligations**

The Subscriber Agreement is included as Appendix B.

### **2.2 Publication and Repository**

The Colby College CA website is: <http://www.colby.edu/CPS>

The CRL repository contains X.509 version two (2) CRLs in accordance with the PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL profile" [RFC2459] in {DER,PEM} format on <http://www.colby.edu/CRL/>.

## **3.0 Identification and Authentication**

### **3.1 Need for Names to Be Meaningful**

The Subject and Issuer name contained in a certificate must be meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.

The organization name component is included in the Distinguished Name (DN) and it is the official name of the Organization/Entity.

For other certificates the name structure shall be:

C=US, O=Colby College, CN=official certificate name.

If the certificate is a server certificate the CN is named as the username of the person defined in our central personnel user-ID (uid) database, Colby CARS Database.

### **3.2 Method to Prove Possession of Private Key**

Certificate requests submitted to the CA must be PKCS#10 requests or other cryptographically equivalent forms where proof of possession of the private key is ensured.

### **3.3 Authentication of Individual Entity**

The CA will authenticate users who apply for certificates to the same level of certainty that any user account login provides. This will be done through automated means by making use of a standard system login authentication method.

### **3.4 Authentication for Routine Renewal of Certificates**

No online renewal requests can be made at this point in time. The routines and authentication methods for signing a renewal request are the same as for subscribing for a certificate.

### **3.5 Authentication of Revocation Request**

The revocation of certificates may be performed after communication with the Colby College CA, the Subscriber or the Colby College CA. The revocation request can be:

- Written request (paper).
- Trusted electronic request (PKCS #7).
- Other trusted communications.

The requestor of a revocation must represent the organization/entity which sponsors the certificate or represent a higher level of responsibility and sponsor in the Colby College CA. An identification of the revocation requestor is made and is verified and controlled by a CASO (Certificate Authority Supervisory Officer) or CAO (Certificate Authority Officer) of the Colby College CA.

## **4.0 Operational Requirements**

### **4.1 Application for a Certificate**

The CA or CAO will issue certificates to eligible applicants whose identities have been authenticated by the methods described in section 3 of the CPS. The CA or CAO will refuse certificate applications when the user authentication fails or in cases where a valid certificate has already been issued and already exists.

A certificate application form including a subscriber agreement is published on the Colby College CA Website (<http://www.colby.edu/CPS>).

This form, together with a certificate request shall be delivered to the CAO. The CAO shall print the electronic request after verification of consistence on the printed request note all requirements as specified in CP 4.1

For a server, the subscriber must have a written authorization from the head of the department.

The identity of the subscriber must be verified using an approved and valid photo-id.

The subscriber shall include:

- Agreement to publish certificate.
- Consent to gather information.

### **4.2 Certificate Revocation**

#### **4.2.1 Circumstances for Revocation**

A certificate will be revoked in situations where:

- Certificate subscriber or entity no longer meets certificate eligibility criteria
- A certificate is no longer usable due to the private key password being lost, forgotten or otherwise unavailable to the subscriber

- The subscriber's private key is compromised or suspected of being compromised
- The subscriber's information in the certificate is no longer accurate
- The subscriber is known to have violated the conditions of the certificate Subscriber Agreement (Appendix B)

#### **4.2.2 Revocation Request Grace Period**

The revocation shall be done within 2 (two) workdays. Any other action taken as a result of a request for revocation of a certificate must be initiated within the same time limit.

#### **4.2.3 Entity Public Certificate is Revoked**

In the event of Colby College CA private key compromise or suspected compromise, the Colby College CA operators must try to contact the PCA and subscribers with any possible means until contact is reached.

In the case of revocation of the Colby College CA certificate, the following steps must be taken:

- Inform the PCA and ensure that the CA certificate is included in the PCA CRL.
- Inform all Colby College CA subscribers using individual and group emails.
- Publish information about the revocation on the public CRL list, located at <http://www.colby.edu/CRL>
- Contact individual subscribers via phone/voicemail if necessary.

#### **4.2.4 CSS Publishing Frequency**

If a certificate is revoked, the on-line CRL shall be updated during the same work day.

### **4.3 Recorded Events**

The Colby College CA personnel shall log the following in a system log or repository:

- issued certificates
- issued CRLs
- certificate requests
- certificate revocation requests
- access to the CA server(s)

In addition to this, standard machine logs (syslog, messages) shall be kept according to Colby College ITS policy.

#### **4.3.1 Frequency of Processing Audit Logs**

The CASO shall periodically review the audit logs and note significant events in an audit log summary.

### **4.4 Records archival**

Backups are kept on removable media in a separate location. They are put in a safe whose key is kept by CAO #1, CAO #3 and CAO #5.

#### **4.5 Secure Facility after a Natural or Other Type Disaster**

Primary computer system and backup system are located at two physically separate sites. Both sites will store removable media containing the CA private key. Removable storage devices containing operating system and application software are stored at both sites. Monthly backups are stored at both sites.

Backup of the CA site excluding the private key are stored on removable media and is taken after every completed change event and stored at the primary site. All backups (hard drives, CDs, DVDs and USB memory sticks) are stored locked in safes separated according to the directives stated in this CPS.

### **5.0 Physical, Procedural and Personnel Security**

#### **5.1 Site Location, Construction and Physical Access**

The RootCA system is a standalone machine with no network access. Transfers of keys are accomplished via removable media.

The public Certificate Authority (CA) is a subordinate CA with automated certificate transfers to the directory masters and web servers for manual certificate generation.

The Colby College CA private key is stored on removable media, physically separated from other data in the CA system. Swap space is encrypted to make recovery of the private key from swap space impossible.

The Colby College CA system's media and the Colby College CA private key are stored in two different safes on the Colby College campus. Access to these safes is restricted to selected staff members of Colby College ITS staff.

When not in use, the private key will be kept in the private key safe. Access to this safe is restricted only to CAO #1, CAO#3, and CAO #5.

Access to the safe containing the CC CA system's other media is restricted to only CAO #2, CAO #3 or CAO #6, Access to the CA system is logged by them. The key to this safe is kept by CAO #2, CAO #4 and CAO #6.

The password to the Colby College CA private key is divided into two parts.

#### **5.2 Trusted roles**

As a complement to the CAO role, there is a new role of Advisory CAO (ACAO). An ACAO can assume the role of a CAO for all purposes, except creating certificates and handling key information. The role of the ACAO may be combined with the role of CASA but not with the role of CASO. An ACAO shall not have knowledge of (any part) of neither the private key nor credentials protecting the private key.

#### **5.3 Number of Person Required per Task**

## Certificate Practice Statement for Colby College CA

CASO: 1

There is only one CASO.

CAO: 5

The CAOs are numbered #1, #2, #3, #4, and #5.

The password to the Colby College CA private key is divided in two parts. CAO#1, CAO #3 and CAO#5 are in possession of the first part and CAO #2 and #4 are in possession of the second part.

### **5.4 Background, Qualifications, Experience, and Clearance Requirements**

The personnel administrating and operating the Colby College CA site must be employees at Colby College. The Personnel must also have earned the trust of and be loyal to the College.

## **6.0 Technical Security Controls**

### **6.1 CA Private Signing Key**

The Colby College CA private key will be stored on removable media and kept in a locked safe while not in use.

### **6.2 Network Security Controls**

The Colby College Root CA server will never be connected to the network. The Colby College CA website is kept on a networked computer. This computer presents public information on the web. Administrative access to this computer is restricted and monitored.

### **6.3 Life-Cycle Security Assurance**

The Colby College CA server(s) will be monitored and maintained by the CA personnel (see Appendix A).

## **Appendix A: CA Personnel**

Certificate Authority Supervisory Officer (CASO):

Rurik Spence

Certificate Authority Officers (CAO):

#1 David Cooley

#2 Jeff Earickson

#3 Keith McGlaufflin

#4 Daniel Siff

#5 Rurik Spence

## Appendix B: Subscriber Agreement

The Subscriber is notified of the importance of the Colby College CA by being informed about the obligations and responsibilities the Subscriber and the Relaying party. The Subscriber confirms having understood this obligations and responsibilities and agreed to it.

The Subscriber shall be informed that a certificate is issued to an individual, even if the Subject is an institute or a role, and the private key is personal.

The Subscriber shall be informed about the information that must be presented with a request and give it's consent to gather this information about the Subscriber needed to complying with the policy. The Subscriber shall also be informed that this information may be transferred across borders.

The Subscriber is informed about the means to communicate with the CA and the RA using the defined email address, which is stated in the CPS or can be accessed through the Colby College CA web site:  
<http://www.colby.edu/CPS>

Other means to communicate is also notified to the Subscriber, which is stated in the Colby College CA web site as well as information about contact personal.

The Subscriber agrees to:

- All information provided by the Subscriber and the representations the Subscriber will make in applying for a certificate are true.
- Have understood the importance of the Colby College Certificate Authority.
- Have understood the responsibility and obligation of a Subscriber.
- Have not and will not allow anyone access to the private key that will be associated with the certificate requested.
- If any information provided by the Subscriber is changed the Subscriber must contact the CA Administrator about the changes.
- If the event, or suspicion of, that the security of the private key is compromised the CA Administrator will be informed. The certificate and private key will then be removed within one working day of being informed that is has been revoked.
- Have understood and comply with all Colby College ITS policies.

The Personnel administrating a web server will agree to:

- Having authority to and accept responsibility for ensuring that anyone who performs administration functions on the web server for which a Colby College CA certificate is issued is fully informed of the requirements for use of the certificate and they agree to use the certificate exclusively for authorized and legal purpose and that is consistent with this policy.