

**Step-by-Step**  
**The CREN Certificate Authority Application Process**  
2/10/00

**I. Persons Involved in the Application Process:**

- (1) **CREN Member Representative** - The institutional member representative for CREN who completes the CREN CA Application Form.
- (2) **Certificate Authority Executive Officer (CAEO)** - An executive officer at the institution who signs the application accepting the conditions of the CREN Certificate Authority service.
- (3) **Institution Certificate Authority Technical Contact (ICATC)** - The technical contact at the applying institution who will issue the Institutional Certificate request and accept the CREN Institutional Certificate.
- (4) **CREN Admin Contact** – The person at CREN who communicates with the various Institutional Representatives to ensure the integrity of the registration process. The primary role of the CREN Admin Contact is to ensure that CREN is communicating with the correct CREN Member Representative at the Institution as well as the correct CAEO and ICATC.
- (5) **CREN Registration Technical Contact (CRTC)** – The person at CREN who will oversee the actual signing of the Institution’s Certificate by CREN. Note: This role will initially be delegated to a person at MIT.
- (6) **CREN Monitor** – The CREN Monitor oversees the entire process to ensure it is properly documented and carried out.

**II. The Application Process**

The application process for a CREN Institutional Certificate has two phases:

- Application and registration process that validates the Institutional Representatives, and sets up secure communication channels.
- Request, issuance and acceptance of the Institutional Certificate

Note: PGP software is used temporarily for the establishment of secure communications between individuals during these application processes. The PGP Personal Public Keys that are distributed and signed during the application process are not to be confused with the Public Keys being generated for inclusion in the CREN Root Certificate or the Institutional Certificates.

## **Phase 1: Application and Registration Process**

The institution and CREN agree to establish a Certificate Authority Subscriber service relationship. The initial point of contact is the CREN member representative on record as the CREN Member Representative. The CREN Member Rep contacts the CREN Admin Contact with a request to establish a Certificate Authority Service relationship between their institution and CREN.

### **Phase 1: Step 1: Preparing to Complete the Application Form**

In preparation for completing the application form, the CREN member representative meets with a management group at the institution who is responsible for digital certificates for faculty, staff and students on their campus to determine the individuals who will be the institutional contacts for the Certificate Authority service with CREN. (Note: The process for designating the individuals may vary widely from campus to campus. The important goal to be achieved is understanding and participation in how the CREN certificate will be used in providing services to the campus community, agreement on who the institutions' contacts will be, and agreement on the Certificate Authority policies on campus.)

### **Phase 1: Step 2: The Application Form**

The CREN member rep completes the Certificate Authority Service Application Form, in which he/she:

- (a) Requests approval for the institution to become a subscriber to the CREN CA service,
- (b) Designates the Certificate Authority Executive Officer (CAEO) who will sign the application accepting the conditions of the CREN Certificate Authority service, and
- (c) Designates the person who will be the Institutional CA Technical Contact (ICATC) who will be responsible for issuing the institutional certificate request and accepting the CREN institutional certificate on behalf of the institution.
- (d) Communicates with the CAEO to ensure the signing of the application form by the CAEO.

Then the Member Rep sends the application to CREN by fax. The CREN Admin Contact sends an email to the CREN Member Rep and copies the CREN Monitor and the ICATC, notifying

them that the Certificate Authority Application has been received. The template which follows will be the appropriate structure for the email.

## **1.2 Email Template to Respond to the Certificate Authority Application**

Subject: "Institution Name: Certificate Authority Application Received"  
To: CREN Member Rep  
From: CREN Admin Contact  
Cc: CREN monitor, CAEO and ICATC

Message:

"This is to acknowledge receipt of "Institution Name" application for the Certificate Authority Service for Higher Education by CREN. Another message will follow in 5 - 10 business days approving or not approving this application."

### **Phase 1: Step 3: Contacting the Member Rep and Validating Contacts**

After the CREN office has received the application form, the CREN Admin Contact reaches the CREN Member Representative via the institution switchboard to verify that the Member Rep, the Certificate Authority Executive Officer (CAEO) and the Institution's Certificate Authority Technical Contact (ICATC) are all aware of their roles in the application and certificate issuance process.

### **Phase 1: Step 4: Contacting the Certificate Authority Executive Officer**

CREN Admin Contact then reaches the person who is to be the Certificate Authority Executive Officer (CAEO) by going through the institution's switchboard to reach the office of the CAEO. The CREN Admin Contact must speak directly with the CAEO.

### **Phase 1: Step 5: Review of the Application**

The CREN Admin Contact then reviews the application for accuracy and completeness, including the statement of assurance of the existence of appropriate certificate authority practices and policies on the campus. The CREN Admin Contact requests that a copy of the institution's certificate authority practice and policies statement be sent to the CREN Admin contact, if such a document is available. [Over time, CREN and the initial community of higher education CREN CA users will develop, and distribute to the community samples of recommended campus CA policy statements.]

## **Phase 1: Step 6: Approval or Denial of the Application**

CREN shall approve or not approve the request for the CREN Certificate Authority Service, making a reasonable effort to approve or not approve such applications within 5 – 10 business days. The CREN Admin Contact then sends an email to the CREN Member Rep, the CA Executive Officer, and the Institution CA Technical Contact that the institution's request for the Certificate Authority service has been approved. The subject heading for this email will be "Institution Name: CA Application Approved " or "Institution Name: CA Application Not Approved." This message is also copied to the CREN Monitor. (Note: If the request for a certificate is coming from a department or college within an institution, this is noted as "Institution-Subgroup Name" in all the subject headings. All applications for the CREN Certificate Authority service must come from the CREN Member Rep.)

### **1.6 Email Template to Approve or Not Approve an Institution's Certificate Authority Service Application.**

Subject: "Institution Name: CA Application Approved." Or "Institution Name: CA Application Not Approved.  
To: CREN Member Rep  
From: CREN Admin Contact  
Cc: CREN Monitor, CAEO, and ICATC

Message:

“This message is to notify you that [Institution’s name] application for CREN’s Certificate Authority Service has been approved.

“The next step is the validation of [Institution’s name] Technical Contact and the exchanging of Personal PGP Public Keys. In preparation for the second part of this step, you may refer to <http://www.cren.net/cren/caindex.html> for the instructions in setting up PGP on your system.

Note: PGP software is used to set up a secure communications channel between individuals during the application process. This secure communications channel is to be maintained for use if the digital certificates/PKI communication should become compromised. The Personal PGP Public Keys distributed and signed during the application process are not to be confused with the Public Keys being generated for inclusion in the CREN Root Certificate or the Institutional Certificate.

“Another email will follow that will contain my Personal PGP Public Key. Should you have any questions, please do not hesitate to contact me.”

\*\*\*\*\*

Note: If for any reason the application for certificate authority service is not approved, the following email will be sent.

"This message is to notify you that the [Institution's name] application for CREN's Certificate Authority Service has not been approved. I will contact you to discuss any next steps."

\*\*\*\*\*

### **Phase 1: Step 7: Validation of the Institution CA Technical Contact (ICATC) and Setting Up a Secure Communication Channel**

Upon approval of the application, CREN Admin Contact then contacts the person who is to be the Institution CA Technical Contact (ICATC) by going through the institution switchboard. This step has multiple substeps for the setting up of a secure communication channel between the Institution CA Technical Contact and the CREN Admin Contact.

The recommended means for setting up this secure communication is via PGP - signed email. Instructions on how to use PGP and additional step-by-step instructions are available on the network, by going to <http://www.cren.net/cren/caindex.html> and selecting the PGP instruction link. Once the Institutional CA Technical Contact (ICATC) is ready to use PGP, having installed PGP on his/her system, and generated a PGP Personal Public/Private Key pair, he/she contacts the CREN Admin Contact.

The CREN Admin Contact and the Institutional CA Technical Contact (ICATC) exchange PGP Personal Public Keys and then each signs the PGP Personal Public Key of the other after verifying the fingerprints of the Keys. The fingerprint is a unique series of numbers generated when the key is created. A key's fingerprint can be viewed by opening the PGPkey application, highlighting a key, and choosing "Properties" from the Keys menu.

The instructions for exchanging PGP Personal Public Keys are as follows.

#### **Phase 1: 7.1 Exchange of Personal PGP Public Keys**

- The CREN Admin Contact sends ICATC his/her PGP Personal Public Key with the standardized subject heading "Institution Name: CREN Admin Contact Personal PK "

- ICATC sends PGP Personal Public Key to CREN Admin Contact with the standardized subject heading "Institution Name: ICATC Personal PK." The ICATC also copies the institution's member rep.

### **1.7.1.a Email to Send the CREN Admin Contact's Personal PGP Public Key to the ICATC**

Subject: "Institution Name: CREN Admin Contact Personal PGP Public Key"  
To: ICATC  
From: CREN Admin Contact  
Cc: CREN Monitor

Message:

"This message contains the Personal PGP Public Key of the CREN Admin Contact. You will want to put this on your personal PGP keyring. You may do this in one of two ways:

If you have an email system that supports PGP, simply click the "Key and Envelop" button in your email application. This will cause the CREN Admin Contact's Public Key in this message to be copied and stored on your personal PGP Public keyring.

Alternatively, you may copy the block of text that follows and paste it into the PGP keys window.

"The next step is for you to send me your Personal PGP Public Key, and to copy your institution's Member Rep on this email. When I receive your Personal PGP Public Key, I will be calling you to exchange fingerprints. The fingerprint is a unique series of numbers generated when the personal PGP key pair is created. You can view your PGP key's fingerprint by opening the PGP Key application, highlighting your key, and choosing "Properties" from the Keys menu."

### **1.7.1 b Email for the Institution's Certificate Authority Technical Contact (ICATC) to send his/her Personal PGP Public Key to the CREN Admin Contact**

Subject: "Institution Name: ICATC Personal PGP Public Key"  
To: CREN Admin Contact  
From: Institution's Certificate Authority Technical Contact (ICATC)  
Cc: CREN Monitor, CREN Member Rep and CREN Registration Technical Contact (CRTC)

Message:

"This message contains the Personal PGP Public Key of the ICATC for [Institution's Name]"

I understand that the next step is for us to exchange fingerprints of our personal PGP public keys. We will do this via phone. Please call [Institution's name]'s switchboard at [phone number] and ask to be transferred to me.

## **Phase 1: 7.2 Exchange of Fingerprints and the Signing of the Personal PGP Public Keys**

- The CREN Admin Contact calls the ICATC through the institution switchboard and they exchange fingerprints via phone.
- After verifying the fingerprints, CREN Admin Contact signs ICATC's PGP Personal Public Key.
- After verifying the fingerprints, ICATC signs CREN Admin Contact 's PGP Personal Public Key.

## **Phase 1: 7.3. Forwarding of ICATC Public Key to the CREN Registration Technical Contact along with authority to issue a certificate.**

- Upon verification of the ICATC PGP Personal Public Key, the CREN Admin Contact forwards the signed ICATC PGP Personal Public Key to the CREN Registration Technical Contact (CRTC) and copies the CREN Monitor.
- The CREN Admin Contact then forwards a copy of the CREN Registration Technical Contact's PGP Personal Public Key to the ICATC.
- The CREN Admin Contact sends a PGP Signed Message to the CREN Registration Technical Contact identifying the ICATC as being authorized to send in a Certificate Request message and also indicating that the institution's application to have a Certificate signed has been approved.

### **1.7.3 a Email Template for the CREN Admin Contact to send to the CREN Registration Technical Contact (CRTC) the PGP Public Key of the ICATC and the message that an institution is approved and that the institution's technical contact is ready to proceed with setting up a secure channel with the CRTC.**

Subject: "Institution Name: ICATC Personal PGP Public Key"  
To: CREN Registration Technical Contact (CRTC)  
From: CREN Admin Contact  
Cc: CREN Monitor and ICATC  
Security: Signed with CREN Admin's Personal PGP Public Key

Message:

"Below is the PGP Personal Public Key of [fill in ICATC's name], the ICATC for [Institution name], signed by me." This message also confirms that [fill in ICATC's name] is authorized to send in a Certificate Request message on behalf of [institution name]. [Name of institution]'s CA application has been approved.

“I will also be forwarding a copy of your PGP Public Key to [fill in ICATC’s name].

“After you and the ICATC set up a secure channel with PGP, the next step is for [institution name]’s ICATC to send you the official Certificate Request, and to copy the CREN Monitor and the CREN Admin Contact. The ICATC should use the standard subject heading of ‘Institution Name: Institutional Certificate Request’ and include it in a signed PGP email message. The message should conform to the Internet Standard RFC 2511. This standard specifies that the Certificate Request contain the following parts:

1. Message requesting that CREN generate a CREN institutional certificate for the institution.
2. Name of the institution in the following X.500 format:  
/C=Country/SP=State/O=Institution Name Spelled Out (for example, the name for MIT would be: /C=US/SP=Massachusetts/O=Massachusetts Institute of Technology)
3. The institution’s Public Key.
4. A pointer to the CREN Certification Practices Statement  
<http://www.cren.net/cren/ca/crencps.doc>.”

### **1.7.3 b Email Template for the CREN Admin Contact to send the PGP Public Key of the CRTC to the ICATC for the setting up of the secure channel**

Subject: CREN Registration Technical Contact (CRTC) Personal PGP Public Key”  
To: Institution Name: ICATC  
From: CREN Admin Contact  
Cc: CREN Contact Registration Technical Contact (CRTC)  
Security: Signed by CREN Admin Contact’s Personal Public PGP Key

Message:

“Below is the Personal PGP Public Key of the CRTC. The next step is for you to exchange fingerprints of your personal PGP Public Keys. You can do this via phone. Please call the CRTC at [Phone Number] to do this.”

### **Optional: Exchange of Test Messages to Verify Valid PGP Signatures**

[If desired, the CREN Admin Contact and Institution Certificate Authority Technical Contact (ICATC) can exchange test messages to add an additional level of assurance that each others’ signatures and keys are valid.]

- CREN Admin Contact sends a signed (and optionally encrypted) test message to ICATC — ICATC’s PGP Personal Public Key has been signed by CREN Admin Contact — with the subject heading: "Institution Name: Verify Valid PGP Personal PK Signature of CREN Admin Contact"

- ICATC receives this message and checks that he/she can verify and read the message and that the signature of the CREN Admin Contact verifies as valid.
- Then ICATC sends a signed (and optionally encrypted) test message to the CREN Admin Contact — CREN Admin Contact 's PGP Personal Public Key has been signed by ICATC — with the subject heading: "Institution Name: Verify Valid Personal PK Signature of ICATC"
- The CREN Admin Contact checks that he/she can verify the test message from ICATC and that the signature of the ICATC verifies as valid.
- CREN Admin Contact sends a confirmation of the test back to ICATC with the standardized subject heading: " Institution Name: Confirm ICATC PPG Personal PK Signature Verified"

\*\*\*\*\*

With the verification of the signatures through the test messages, the CREN Admin Contact and the Institution Certificate Authority Technical Contact (and the institution) have established a secure email communications channel.

## **Phase 2: Certificate Request, Certificate Issuance, and Acceptance**

This section provides a summary of the process to be used for the request, issuance and acceptance of the Institutional CREN Certificate. The Certificate Authority Request will follow the standard (RFC 2511) from the Internet Engineering Task Force (IETF) X.509 Public Key Infrastructure Working Group.

### **Phase 2: Step 1: Request of Certificate by Institution**

The ICATC sends a request for the Institutional Certificate to the CREN Registration Technical Contact with the standardized subject heading: "Institution Name: Request for Institutional Certificate" in a signed email with a copy to the CREN Admin Contact and the CREN Monitor. (Note: This message will conform to the Internet Standard RFC 2511. For an interim period of time, Certificate Request Messages may be sent in the format output by common Certifying Authority products including Netscape and Apache. It is expected that these products will be updated to generate conformant RFC2511 messages in the future.)

The IETF standard (RFC2511) specifies that the Certificate Request will contain the following parts:

1. Message requesting that CREN generate a CREN digital certificate for the institution.
2. Name of the institution in the following X.500 format:  
/C=Country/SP=State/O=Institution Name Spelled Out. (For example, the name for MIT would be:  
/C=US/SP=Massachusetts/O=Massachusetts Institute of Technology)
3. The institution's public key
4. A pointer to the CREN Certification Practices Statement  
<http://www.cren.net/cren/ca/crencps.doc>

## **2.1 Email Template for the ICATC to request the official CREN Institutional Certificate**

Subject: Institution Name: Request for Institutional Certificate  
To: CREN Registration Technical Contact (CRTC)  
From: ICATC  
Cc: CREN Admin Contact and CREN Monitor  
Security: Signed with the personal PGP key of the ICATC

Message:

"Enclosed in this email is [Institution's Name] official Request for a CREN institutional certificate.

(This message also contains:

Name of the institution in the following X.500 format:

/C=Country/SP=State/O=Institution Name Spelled Out (for example, the name for MIT would be: /C=US/SP=Massachusetts/O=Massachusetts Institute of Technology)

The institution's Public Key.

A pointer to the CREN Certification Practices Statement

<http://www.cren.net/cren/ca/crencps.doc>."

## **Phase 2: Step 2: Verification of the Certificate Request Message**

When the CREN Registration Technical Contact (CRTC) receives the Certificate Request Message, the CRTC verifies two items: the valid signature of the ICATC and the accuracy of the components of the Certificate request. If the message was unsigned, or if problems existed in signature verification, this process may iterate until a valid Certificate Request Message is received by the CRTC. (Note: It is possible that the ICATC may need explicit assistance in representing their institution's name in the X.500 parlance used by Certificates.)

## **Phase 2: Step 3: Issuance of the Institutional Certificate**

The CREN Registration Technical Contact receives the formal Certificate Request and verifies the signature on the message. The CREN Registration Technical Contact also verifies the proper format of the request and if all is in readiness arranges to create a signed Certificate. The exact details of this process are beyond the scope of this document, but include such details as checking the proposed Certificate's validity dates, ensuring a proper serial number and finally ensuring that the signed Certificate is properly recorded in the CREN database of signed certificates. The final Certificate has the following fields:

1. The institution's X.500 name as provided in the request message
2. CREN's X.500 name and CREN listed as the issuer of the certificate
3. The Public Key of the institution as taken from the Request message
4. The range of dates that the Certificate is valid (The initial certificates will be valid for two years.)
5. A unique serial number according to X.509 standards
6. A Digital Signature created with the CREN CA's Private Key

## **Phase 2: Step 4: CREN Certificate Sent to Institution**

The CRTC sends the CREN-signed Institutional Certificate to the ICATC, the Member Rep, the CREN Admin Contact, and the CREN Monitor, via signed PGP email.

### **2.4 Email Template for the CRTC to send the CREN Institutional Certificate to the ICATC at the institution**

Subject: Institution Name: CREN Institutional Certificate  
To: Institution's Certificate Authority Technical Contact (ICATC)  
From: CREN Registration Technical Contact (CRTC)  
Cc: CREN Admin Contact, CREN Monitor, and CREN Member Rep  
Security: This message is to be PGP signed with the CRTC Personal PGP Key.

Message:

"Enclosed in this email is Institution's Name" CREN Institutional Certificate.

"Now that you have received your CREN Institutional Certificate, please accept and validate the certificate by sending a message back to the CRTC, and copying the CREN Monitor, the CREN Admin Contact, and the CREN Member Rep, to confirm that [Institution Name] has accepted the CREN Institutional Certificate. Please use the standardized heading of "[Institution Name] Acceptance of the CREN Root CA Certificate"

The note can read, "This note can act as [Institution Name]'s formal acceptance of the CREN Root CA Certificate. I attest that the Certificate is accurate and functioning correctly."

"When we receive this validation, the CREN Repository of Institutional Certificates will be updated, and the Certificate Authority application process will be complete."

"Thank you for using the CREN Certificate Authority Service."

## **Phase 2: Step 5: ICATC Verifies and Accepts the Institutional Certificate**

The ICATC verifies that the returned Certificate is valid using the published CREN Public Key. The ICATC will also verify that its institution's Public Key correctly appears in the returned Certificate using a direct comparison approach to ensure against an error in processing at CREN. The ICATC verifies its Institutional Certificate and sends a signed PGP message back to the CREN Registration Technical Contact with a copy to the CREN Admin Contact, the Member Rep, and the CREN Monitor, accepting the Certificate with the subject heading: " Institution Name: Certificate Accepted."

### **2.5 Email Template for the ICATC to CRTC to accept the CREN Certificate on behalf of the institution**

Subject: Institution Name: Acceptance of the CREN Institutional Certificate  
To: CREN Registration Technical Contact (CRTC)  
From: Institution's Certificate Authority Technical Contact (ICATC)  
Cc: CREN Admin Contact, CREN Monitor, and CREN Member Rep  
Security: This message is to be signed with the ICATC Personal PGP Key.

Message:

"This note serves as the [Institution Name]'s formal acceptance of the CREN Institutional Certificate, and attests that the Certificate is accurate and functioning correctly."

"I understand that when you receive this validation, that the CREN Repository of Institutional Certificates will be updated, and the Certificate Authority application process will be complete."

## **Phase 2: Step 6: CREN Repository Updated**

The CREN Repository is updated to include this subscriber's Certificate.

**YOU ARE NOW READY TO USE THE CREN Certificate!**

.....

The content of digital certificates are prescribed by the X.509 standard, developed by the International Standards Organization (ISO) and adopted by the American National Standards Institute and the Internet Engineering Task Force. (IETF) The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

RFC 2511: Title: Internet X.509 Certificate Request Message Format

This describes the Certificate Request Message Format (CRMF). This syntax is used to convey a request for a certificate to a Certification Authority (CA) for the purposes of X.509 certificate production. The request will typically include a public key and associated registration information.

The latest version is now X.509v3. The principal elements of a digital certificate are:

- ◆ Version number of the certificate format
- ◆ Serial number of the certificate
- ◆ Signature algorithm identifier
- ◆ Issuer of digital certificate: a certificate authority with URL
- ◆ Validity period
- ◆ Unique identification of certificate holder
- ◆ Public key information