Certificates Signed by CREN Certification Authority

Statement for Relying Parties

Draft Version v. 3 December 10 2001

Introduction

The issue of trust is basic to the purpose of the PKI infrastructure. The confidence in any PKI certificate is directly related to at least three components of a Certification Authority —the trustworthiness and security of the Certification Authority itself, the processes for validating that the Subject of a certificate signing request is legitimately represented by the requesting entity, and the processes for issuing the certificates and making sure they and the corresponding private keys are in the possession of the appropriate entity.

In the case of the CREN Certification Authority the processes are detailed in the Certification Practice Statement (CPS) dated January 27, 2000 that is at the CREN web site at http://www.cren.net. This CPS is a hybrid document containing both certificate policy (CP) and certificate practice statement (CPS) provisions.

The CREN Certification Authority (CA) is the root or "trust anchor" of a hierarchical certification authority. This means that the CREN CA can sign the public keys from other Certification Authorities such as a campus Certification Authority. When the CREN CA signs the public key, it creates a certificate that contains the public key generated by the campus CA with a Subject Field that contains the name of the campus institution, and an Issuer Field that contains the name of the CREN CA. There is no relationship implied or intended between that Subject Field and any information external to the certificate.

Interpreting the trustworthiness of a CA authority certificate signed by CREN

In the application process for a CREN-signed CA authority certificate, representatives of an institution complete an application form in which they attest that their campus has "procedures in place that appropriately protect the institution's private key for the campus certificate authority service." However, no specific details of how this is accomplished are required.

The application includes the names of three official representatives of the institution. Those three representatives are the (1) CREN member rep on file with CREN office, (2) the Certificate Authority Executive Officer, and (3) the Certificate Authority Technical Contact. All three of these representatives are validated in an identification and authorization (I & A) process to ensure that they have the right to request a certificate with that institution's name in the Subject field.

When CREN signs the public key of an institution, it is attesting to the fact that that request came from the institution whose legal name is in the Subject Field, that official representatives of that institution attested to having appropriate practices in place for operation and management of a certification authority, and that the CREN-signed CA authority certificate for that institution was delivered to a representative of that institution who also has access to the corresponding private key.

Relying Parties should verify that they have the valid CREN CA root certificate to validate the institutional certificates. Relying parties can request a copy of the CREN root directly from CREN or download the CREN root certificate from www.cren.net and compare the fingerprints of the downloaded certificate with those of the certificate on the site.

Once a certificate is issued for the default validity period of five years for the campus CA, CREN takes no further action to monitor the use of the certificate nor its continued validity. If requested, CREN **may** investigate the validity of a CREN-issued certificate and **may** issue a revocation if warranted.

Interpreting the trustworthiness of a certificate signed by a Campus CA authorized by CREN

Before relying on a certificate signed with the private key associated with a CREN-signed CA authority certificate Relying Parties should refer to the Certificate Policy and Certification Practices Statements under which the campus CA operates.

There is a generic PKI-Light Certificate Policy and a generic PKI-Light Certificate Practice Statement that may become widely used. These certificate policies are intended to address the bulk of questions about the processes by which students, staff and faculty are validated and the common practices for operating a campus CA for applications with very low risk or liability implications.

The certificates issued by the campus will have a URL pointing to their campus CPS in the CPSuri field. The CPS in turn will reference an on-line copy of the campus CA's CP.

Summary

When a Relying Party receives a valid certificate signed by CREN-authorized institutional CA, it can be assured that that certificate has been issued by the institution or entity in the Subject field. Relying Parties that want more validation

about any certificate should access related campus CA policy and/or practices statements, or campus directory/database information.