PowerTalk: Obtaining Certificates (7/96)

Article Created: 6 September 1994
Article Reviewed/Updated: 5 July 1996

TOPIC ---

The process by which an end-user obtains a Certificate involves three steps.

1) Completion of a Certificate Signing Request.

2) Validation of identity (as stated in the Certificate Signing Request) by an authorized entity.

3) Issuance of the Certificate based on the validated Certificate Signing Request.

DISCUSSION ---

Overview

Every PowerTalk package in the U.S.A. will include a voucher for one Signer file.

RSA Data Security Inc. is the root of all public key certificate sets. Individual users will be able to obtain a public key certificate directly from RSA. Negotiations are underway to establish a method for overseas customers to receive certificates. The Tech Info Library article titled "Locating Vendor Information" can help you search for RSA Data Security's address and phone number.

Large corporations and other organizations can contract with RSA to issue certificates to their employees. By convention, the certificate chain can only be two levels deep. Therefore, it will not be possible for a corporation authorized by RSA to issue certificates, to in turn, authorize another organization to issue certificates.

The DigiSign Utility is used to create a Signer Approval Request and the unapproved Signer file. Once a Signer Approval has been issued by the issuing authority, the DigiSign Utility will again be used to merge the unapproved Signer file with the Signer Approval file to create a final Signer file.

Completion of a Certificate Signing Request

Every Public Key Cryptography Standards (PKCS) or Internet Privacy Enhanced Mail (PEM) compliant application includes the functionality to generate an electronic Certificate Signing Request. The Certificate Signing Request (hereafter, "Request") includes the necessary information to issue a Certificate.

The process of completing the Request starts with the generation of an RSA key pair. This functionality is included in the application. Typically, the user will then provide some personal identification information and choose an appropriate distinguished name, which will make the Certificate unique.

Validation of a Certificate Signing Request

The next step in the process is validation of the identity of the end-user with the information contained in the Request. How this is done depends upon the type of Certificate Issuing relationship that an organization or individual has with RSA. The possible relationships are Certificate Issuing System (CIS)-Issuer, Co-Issuer, or Unaffiliated.

Begin_Table

CIS-Issuer	The end-user takes the Request, with proper ID, to the Organizational Notary (ON) to be validated. The ON will use internal procedures to confirm the authenticity of the user's identifying information and the uniqueness of their distinguished name.
Co-Issuer	The process is the same as that for a CIS-Issuer.
Unaffiliated	The end-user takes the Request, with proper ID, to be notarized by an official Notary Public.

End_Table

Fulfilling a Certificate Signing Request

The end-user now has a Request that has been completed and validated. The final step is fulfilling the Certificate Signing Request by issuing the Certificate based on the Request. Again, how this is done depends upon the type of Certificate Issuing relationship that an organization enters into with RSA.

Begin_Table

CIS-Issuer	The validated Request is taken to the Certificate Issuer (CI), within the organization, who then issues the Certificate using the Certificate Issuing System (CIS).
Co-Issuer	The ON sends the validated Request to the VeriSign Inc. which then issues the Certificate on behalf of the organization.
Unaffiliated	The validated Request is mailed to VeriSign Inc. whose staff will verify that the Notary Public stamp/seal is valid, verify uniqueness of the distinguished name,

generate the Certificate (if the request is valid) and send the user the Certificate on diskette or via E-mail.

End_Table

Generating a Certificate

An example of how an unaffiliated Certificate will be generated in conjunction with typical commercial software (call it Application X), is described below.

1) Application X, a security-aware application, has been developed with one of RSA's toolkits. This application includes functionality for the generation of RSA key pairs as well as Certificate Signing Request forms.

2) The end-user (let's call him Kurt) uses the application's key generation utility on his computer to generate his own RSA key pair, and also inputs personal identifying information to be contained in his Certificate.

3) Application X produces a printed paper or electronic form, containing Kurt's public key and personal identifying information (this is his Certificate Signing Request). Kurt takes the form to a Notary Public for notarization.

4) Kurt mails the notarized form to VeriSign Inc. for processing.

5) VeriSign Inc. processes the request as an Unaffiliated Certificate Signing Request. VeriSign Inc.'s staff uses CIS to create a Certificate based on the request.

6) VeriSign Inc. sends the completed Certificate back to Kurt via diskette, or E-mail (via Internet) for use within Application X.

Generation of an end-user Certificate, utilizing RSA's Co-Issuer relationship, differs from the process described above in that there must be an Organizational Notary (ON) within the organization that completes step 5 rather than RSA. For organizations with a CIS on-site, steps 5 and 6 are completed by the organizations ON and CI, respectively.

Article Change History:
10 Apr 1996 - Updated article.
18 Oct 1995 - Added how to contact RSA Data Security Inc.
18 Jan 1995 - Added Overview section.

Keywords: supt

==========

19960708 06:59:23.00

Tech Info Library Article Number: 16207