Network Working Group
Request for Comments: 2314
Category: Informational

B. Kaliski
RSA Laboratories East

March 1998

PKCS #10: Certification Request Syntax
Version 1.5

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Overview

This document describes a syntax for certification requests.

1. Scope

A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a certification authority, who transforms the request to an X.509 public-key certificate, or a PKCS #6 extended certificate. (In what form the certification authority returns the newly signed certificate is outside the scope of this document. A PKCS #7 message is one possibility.)

The intention of including a set of attributes is twofold: to provide other information about a given entity, such as the postal address to which the signed certificate should be returned if electronic mail is not available, or a "challenge password" by which the entity may later request certificate revocation; and to provide attributes for a PKCS #6 extended certificate. A non-exhaustive list of attributes is given in PKCS #9.

Certification authorities may also require non-electronic forms of request and may return non-electronic replies. It is expected that descriptions of such forms, which are outside the scope of this document, will be available from the certification authority.

The preliminary intended application of this document is to support PKCS #7 cryptographic messages, but is expected that other applications will be developed.

2. References

PKCS #1 RSA Laboratories. PKCS #1: RSA Encryption Standard. Version 1.5, November 1993.

PKCS #6 RSA Laboratories. PKCS #6: Extended-Certificate Syntax. Version 1.5, November 1993.

PKCS #7 RSA Laboratories. PKCS #7: Cryptographic Message Syntax. Version 1.5, November 1993.

PKCS #9 RSA Laboratories. PKCS #9: Selected Attribute Types. Version 1.1, November 1993.

RFC 1424 Kaliski, B., "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services," RFC 1424, February 1993.

X.208 CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.

X.209 CCITT. Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

X.500 CCITT. Recommendation X.500: The Directory-- Overview of Concepts, Models and Services. 1988.

X.501 CCITT. Recommendation X.501: The Directory-- Models. 1988.

X.509 CCITT. Recommendation X.509: The Directory-- Authentication Framework. 1988.

3. Definitions

For the purposes of this document, the following definitions apply.

AlgorithmIdentifier: A type that identifies an algorithm (by object identifier) and any associated parameters. This type is defined in X.509.

Attribute: A type that contains an attribute type (specified by object identifier) and one or more attribute values. This type is defined in X.501.

ASN.1: Abstract Syntax Notation One, as defined in X.208.

BER: Basic Encoding Rules, as defined in X.209.

Certificate: A type that binds an entity’s distinguished name to a public key with a digital signature. This type is defined in X.509. This type also contains the distinguished name of the certificate issuer (the signer), an issuer- specific serial number, the issuer’s signature algorithm identifier, and a validity period.

DER: Distinguished Encoding Rules for ASN.1, as defined in X.509, Section 8.7.

Name: A type that uniquely identifies or "distinguishes" objects in a X.500 directory. This type is defined in X.501. In an X.509 certificate, the type identifies the certificate issuer and the entity whose public key is certified.

4. Symbols and abbreviations

No symbols or abbreviations are defined in this document.

5. General overview

The next section specifies certification request syntax.

This document exports one type, CertificationRequest.

6. Certification request syntax

This section gives the syntax for certification requests.

A certification request consists of three parts: "certification request information," a signature algorithm identifier, and a digital signature on the certification request information. The certification request information consists of the entity’s distinguished name, the entity’s public key, and a set of attributes providing other information about the entity.

The process by which a certification request is constructed involves the following steps:

1. A CertificationRequestInfo value containing a distinguished name, a public key, and optionally a set of attributes is constructed by an entity.

2. The CertificationRequestInfo value is signed with the entity’s private key. (See Section 6.2.)

3. The CertificationRequestInfo value, a signature algorithm identifier, and the entity’s signature are collected together into a CertificationRequest value, defined below.

A certification authority fulfills the request by verifying the entity’s signature, and, if it is valid, constructing a X.509 certificate from the distinguished name and public key, as well as an issuer name, serial number, validity period, and signature algorithm of the certification authority’s choice. If the certification request contains a PKCS #9 extended-certificate-attributes attribute, the certification authority also constructs a PKCS #6 extended certificate from the X.509 certificate and the extended-certificate-attributes attribute value.

In what form the certification authority returns the new certificate is outside the scope of this document. One possibility is a PKCS #7 cryptographic message with content type signedData, following the degenerate case where there are no signers. The return message may include a certification path from the new certificate to the certification authority. It may also include other certificates such as cross-certificates that the certification authority considers helpful, and it may include certificate-revocation lists (CRLs). Another possibility is that the certification authority inserts the new certificate into a central database.

This section is divided into two parts. The first part describes the certification-request-information type CertificationRequestInfo, and the second part describes the top-level type CertificationRequest.

Notes.

1. An entity would typically send a certification request after generating a public-key/private-key pair, but may also do so after a change in the entity’s distinguished name.

2. The signature on the certification request prevents an entity from requesting a certificate with another party’s public key. Such an attack would give the entity the minor ability to pretend to be the originator of any message signed by the other party. This attack is significant only if the entity does not know the message being signed, and the signed part of the message does not identify the signer. The entity would still not be able to decrypt messages intended for the other party, of course.

3. How the entity sends the certification request to a certification authority is outside the scope of this document. Both paper and electronic forms are possible.

4. This document is not compatible with the certification request syntax for Privacy-Enhanced Mail, as described in RFC 1424. The syntax in this document differs in three respects: It allows a set of attributes; it does not include issuer name, serial number, or validity period; and it does not require an "innocuous" message to be signed. The syntax in this document is designed to minimize request size, an important constraint for those certification authorities accepting requests on paper.

6.1 CertificationRequestInfo

Certification request information shall have ASN.1 type CertificationRequestInfo:

```
CertificationRequestInfo ::= SEQUENCE {
  version Version,
  subject Name,
  subjectPublicKeyInfo SubjectPublicKeyInfo,
  attributes [0] IMPLICIT Attributes }

Version ::= INTEGER

Attributes ::= SET OF Attribute
```

The fields of type CertificationRequestInfo have the following meanings:

- version is the version number, for compatibility with future revisions of this document. It shall be 0 for this version of the document.

- subject is the distinguished name of the certificate subject (the entity whose public key is to be certified).

- subjectPublicKeyInfo contains information about the public key being certified. The information identifies the entity’s public-key algorithm (and any associated parameters); examples of public-key algorithms include X.509’s rsa and PKCS #1’s rsaEncryption. The information also includes a bit-string representation of the entity’s public key. For both public-key algorithms just mentioned, the bit string contains the BER encoding of a value of X.509/PKCS #1 type RSAPublicKey.

- attributes is a set of attributes providing additional information about the subject of the certificate. Some attribute types that might be useful here are defined in PKCS #9. An example is the challenge-password attribute, which specifies a password by which the entity may request that the certificate revocation. Another example is the extended-certificate-attributes attribute, which specifies attributes for a PKCS #6 extended certificate.

6.2 CertificationRequest

A certification request shall have ASN.1 type CertificationRequest:

```
CertificationRequest ::= SEQUENCE {
  certificationRequestInfo CertificationRequestInfo,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature Signature }

SignatureAlgorithmIdentifier ::= AlgorithmIdentifier

Signature ::= BIT STRING
```

The fields of type CertificationRequest have the following meanings:

- certificateRequestInfo is the "certification request information." It is the value being signed.

- signatureAlgorithm identifies the signature algorithm (and any associated parameters) under which the certification-request information is signed. Examples include PKCS #1’s md2WithRSAEncryption and md5WithRSAEncryption.

- o signature is the result of signing the certification request information with the certification request subject’s private key.

The signature process consists of two steps:

1. The value of the certificationRequestInfo field is DER encoded, yielding an octet string.

2. The result of step 1 is signed with the certification request subject’s private key under the specified signature algorithm, yielding a bit string, the signature.

Note. The syntax for CertificationRequest could equivalently be written with the X.509 SIGNED macro:

```
CertificationRequest ::= SIGNED CertificateRequestInfo
```

Security Considerations

Security issues are discussed throughout this memo.

Revision history

Version 1.0

Version 1.0 is the initial version.

Acknowledgements

This document is based on a contribution of RSA Laboratories, a division of RSA Data Security, Inc. Any substantial use of the text from this document must acknowledge RSA Data Security, Inc. RSA Data Security, Inc. requests that all material mentioning or referencing this document identify this as "RSA Data Security, Inc. PKCS #10".

Author’s Address

Burt Kaliski
RSA Laboratories East
20 Crosby Drive
Bedford, MA 01730

Phone: (617) 687-7000
EMail: burt@rsa.com

Full Copyright Statement