Network Working Group
Request for Comments: 1424

B. Kaliski
RSA Laboratories

February 1993

Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services

Status of this Memo

This RFC specifies an IAB standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Acknowledgements

This document is the product of many discussions at RSA Data Security, at Trusted Information Systems, and on the <pem-dev@tis.com> mailing list. Contributors include Dave Balenson, Jim Bidzos, Pat Cain, Vint Cerf, Pam Cochrane, Steve Dusse, Jeff Fassett, Craig Finseth, Jim Galvin, Mike Indovina, Bob Jueneman, Steve Kent, John Lowry, Paul McKenney, Jeff Thompson, and Charles Wu. This document is the product of the Privacy-Enhanced Electronic Mail Working Group.

1. Executive Summary

This document describes three types of service in support of Internet Privacy-Enhanced Mail (PEM) [1-3]: key certification, certificate-revocation list (CRL) storage, and CRL retrieval. Such services are among those required of an RFC 1422 [2] certification authority. Other services such as certificate revocation and certificate retrieval are left to the certification authority to define, although they may be based on the services described in this document.

Each service involves an electronic-mail request and an electronic-mail reply. The request is either an RFC 1421 [1] privacy-enhanced message or a message with a new syntax defined in this document. The new syntax follows the general RFC 1421 syntax but has a different process type, thereby distinguishing it from ordinary privacy-enhanced messages. The reply is either an RFC 1421 privacy-enhanced message, or an ordinary unstructured message.

Replies that are privacy-enhanced messages can be processed like any other privacy-enhanced message, so that the new certificate or the retrieved CRLs can be inserted into the requestor’s database during

normal privacy-enhanced mail processing.

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 through a certification authority's "information" service.

2. Overview of Services

This section describes the three services in general terms.

The electronic-mail address to which requests are sent is left to the certification authority to specify. It is expected that certification authorities will advertise their addresses as part of an "information" service. Replies are sent to the address in the "Reply-To:" field of the request, and if that field is omitted, to the address in the "From:" field.

2.1 Key Certification

The key-certification service signs a certificate containing a specified subject name and public key. The service takes a certification request (see Section 3.1), signs a certificate constructed from the request, and returns a certification reply (see Section 3.2) containing the new certificate.

The certification request specifies the requestor's subject name and public key in the form of a self-signed certificate. The certification request contains two signatures, both computed with the requestor's private key:

1. The signature on the self-signed certificate, having the cryptographic purpose of preventing a requestor from requesting a certificate with another party's public key. (See Section 4.)

2. A signature on some encapsulated text, having the practical purpose of allowing the certification authority to construct an ordinary RFC 1421 privacy-enhanced message as a reply, with user-friendly encapsulated text. (RFC 1421 does not provide for messages with certificates but no encapsulated text; and the self-signed certificate is not "user friendly" text.) The text should be something innocuous like "Hello world!"

A requestor would typically send a certification request after generating a public-key/private-key pair, but may also do so after a

change in the requestor's distinguished name.

A certification authority signs a certificate only if both signatures in the certification request are valid.

The new certificate contains the subject name and public key from the self-signed certificate, and an issuer name, serial number, validity period, and signature algorithm of the certification authority's choice. (The validity period may be derived from the self-signed certificate.) Following RFC 1422, the issuer may be any whose distinguished name is superior to the subject's distinguished name, typically the one closest to the subject. The certification authority signs the certificate with the issuer's private key, then transforms the request into a reply containing the new certificate (see Section 3.2 for details).

The certification reply includes a certification path from the new certificate to the RFC 1422 Internet certification authority. It may also include other certificates such as cross-certificates that the certification authority considers helpful to the requestor.

2.2 CRL Storage

The CRL storage service stores CRLs. The service takes a CRL-storage request (see Section 3.3) specifying the CRLs to be stored, stores the CRLs, and returns a CRL-storage reply (see Section 3.4) acknowledging the request.

The certification authority stores a CRL only if its signature and certification path are valid, following concepts in RFC 1422 (Although a certification path is not required in a CRL-storage request, it may help the certification authority validate the CRL.)

2.3 CRL Retrieval

The CRL retrieval service retrieves the latest CRLs of specified certificate issuers. The service takes a CRL-retrieval request (see Section 3.5), retrieves the latest CRLs the request specifies, and returns a CRL-retrieval reply (see Section 3.6) containing the CRLs.

There may be more than one "latest" CRL for a given issuer, if that issuer has more than one public key (see RFC 1422 for details).

The CRL-retrieval reply includes a certification path from each retrieved CRL to the RFC 1422 Internet certification authority. It may also include other certificates such as cross-certificates that the certification authority considers helpful to the requestor.

3. Syntax

This section describes the syntax of requests and replies for the three services, giving simple examples.

3.1 Certification request

A certification request is an RFC 1421 MIC-ONLY or MIC-CLEAR privacy-enhanced message containing a self-signed certificate. There is only one signer.

The fields of the self-signed certificate (which has type Certificate, as in RFC 1422) are as follows:

version is 0

serialNumber is arbitrary; the value 0 is suggested unless the certification authority specifies otherwise

signature is the algorithm by which the self-signed certificate is signed; it need not be the same as the algorithm by which the requested certificate is to be signed

issuer is the requestor's distinguished name

validity is arbitrary; the value with start and end both at 12:00am GMT, January 1, 1970, is suggested unless the certification authority specifies otherwise

subject is the requestor's distinguished name

subjectPublicKeyInfo is the requestor's public key

The requestor's MIC encryption algorithm must be asymmetric (e.g., RSA) and the MIC algorithm must be keyless (e.g., RSA-MD2, not MAC), so that anyone can verify the signature.

Example:

```
To: cert-service@ca.domain
From: requestor@host.domain

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,MIC-ONLY
Content-Domain: RFC822
Originator-Certificate: <requestor's self-signed certificate>
MIC-Info: RSA,RSA-MD2,<requestor's signature on text>

<text>
-----END PRIVACY-ENHANCED MESSAGE-----
```

3.2 Certification reply

A certification reply is an RFC 1421 MIC-ONLY or MIC-CLEAR privacy-enhanced message containing a new certificate, its certification path to the RFC 1422 Internet certification authority, and possibly other certificates. There is only one signer. The "MIC-Info:" field and encapsulated text are taken directly from the certification request. The reply has the same process type (MIC-ONLY or MIC-CLEAR) as the request.

Since the reply is an ordinary privacy-enhanced message, the new certificate can be inserted into the requestor's database during normal privacy-enhanced mail processing. The requestor can forward the reply to other requestors to disseminate the certificate.

Example:

```
To: requestor@host.domain
From: cert-service@ca.domain

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,MIC-ONLY
Content-Domain: RFC822
Originator-Certificate: <requestor's new certificate>
Issuer-Certificate: <issuer's certificate>
MIC-Info: RSA,RSA-MD2,<requestor's signature on text>

<text>
-----END PRIVACY-ENHANCED MESSAGE-----
```

3.3 CRL-storage request

A CRL-storage request is an RFC 1421 CRL-type privacy-enhanced message containing the CRLs to be stored and optionally their certification paths to the RFC 1422 Internet certification authority.

Example:

```
To: cert-service@ca.domain
From: requestor@host.domain

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,CRL
CRL: <CRL to be stored>
Originator-Certificate: <CRL issuer's certificate>
CRL: <another CRL to be stored>
Originator-Certificate: <other CRL issuer's certificate>
-----END PRIVACY-ENHANCED MESSAGE-----
```

3.4 CRL-storage reply

A CRL-storage reply is an ordinary message acknowledging the storage of CRLs. No particular syntax is specified.

3.5 CRL-retrieval request

A CRL-retrieval request is a new type of privacy-enhanced message, distinguished from RFC 1421 privacy-enhanced messages by the process type CRL-RETRIEVAL-REQUEST.

The request has two or more encapsulated header fields: the required "Proc-Type:" field and one or more "Issuer:" fields. The fields must appear in the order just described. There is no encapsulated text, so there is no blank line separating the fields from encapsulated text.

Each "Issuer:" field specifies an issuer whose latest CRL is to be retrieved. The field contains a value of type Name specifying the issuer's distinguished name. The value is encoded as in an RFC 1421 "Originator-ID-Asymmetric:" field (i.e., according to the Basic Encoding Rules, then in ASCII).

Example:

```
To: cert-service@ca.domain
From: requestor@host.domain

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,CRL-RETRIEVAL-REQUEST
Issuer: <issuer whose latest CRL is to be retrieved>
Issuer: <another issuer whose latest CRL is to be retrieved>
-----END PRIVACY-ENHANCED MESSAGE-----
```

3.6 CRL-retrieval reply

A CRL-retrieval reply is an RFC 1421 CRL-type privacy-enhanced message containing retrieved CRLs, their certification paths to the RFC 1422 Internet certification authority, and possibly other certificates.

Since the reply is an ordinary privacy-enhanced message, the retrieved CRLs can be inserted into the requestor's database during normal privacy-enhanced mail processing. The requestor can forward the reply to other requestors to disseminate the CRLs.

Example:

```
To: requestor@host.domain
From: cert-service@ca.domain

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,CRL
CRL: <issuer's latest CRL>
Originator-Certificate: <issuer's certificate>
CRL: <other issuer's latest CRL>
Originator-Certificate: <other issuer's certificate>
-----END PRIVACY-ENHANCED MESSAGE-----
```

Patent Statement

This version of Privacy Enhanced Mail (PEM) relies on the use of patented public key encryption technology for authentication and encryption. The Internet Standards Process as defined in RFC 1310 requires a written statement from the Patent holder that a license will be made available to applicants under reasonable terms and conditions prior to approving a specification as a Proposed, Draft or Internet Standard.

The Massachusetts Institute of Technology and the Board of Trustees of the Leland Stanford Junior University have granted Public Key Partners (PKP) exclusive sub-licensing rights to the following patents issued in the United States, and all of their corresponding foreign patents:

Cryptographic Apparatus and Method ("Diffie-Hellman")..... No. 4,200,770

Public Key Cryptographic Apparatus and Method ("Hellman-Merkle")..... No. 4,218,582

Cryptographic Communications System and Method ("RSA")..... No. 4,405,829

Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig")..... No. 4,424,414

These patents are stated by PKP to cover all known methods of practicing the art of Public Key encryption, including the variations collectively known as El Gamal.

Public Key Partners has provided written assurance to the Internet Society that parties will be able to obtain, under reasonable, nondiscriminatory terms, the right to use the technology covered by these patents. This assurance is documented in RFC 1170 titled "Public Key Standards and Licenses". A copy of the written assurance dated April 20, 1990, may be obtained from the Internet Assigned Number Authority (IANA).

The Internet Society, Internet Architecture Board, Internet Engineering Steering Group and the Corporation for National Research Initiatives take no position on the validity or scope of the patents and patent applications, nor on the appropriateness of the terms of the assurance. The Internet Society and other groups mentioned above have not made any determination as to any other intellectual property rights which may apply to the practice of this standard. Any further consideration of these matters is the user's own responsibility.

Security Considerations

The self-signed certificate (Section 3.1) prevents a requestor from requesting a certificate with another party's public key. Such an attack would give the requestor the minor ability to pretend to be the originator of any message signed by the other party. This attack is significant only if the requestor does not know the message being signed, and the signed part of the message does not identify the signer. The requestor would still not be able to decrypt messages

intended for the other party, of course.

References

[1] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, DEC, February 1993.

[2] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, BBN, February 1993.

[3] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, TIS, February 1993.

Author's Address

Burton S. Kaliski, Jr.
RSA Laboratories (a division of RSA Data Security, Inc.)
10 Twin Dolphin Drive
Redwood City, CA 94065

Phone: (415) 595-7703
FAX: (415) 595-4126
EMail: burt@rsa.com