Network Working Group
Request for Comments: 2585
Category: Standards Track

R. Housley
SPYRUS
P. Hoffman
IMC

May 1999

Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP

Status of this Memo

Copyright Notice

Abstract

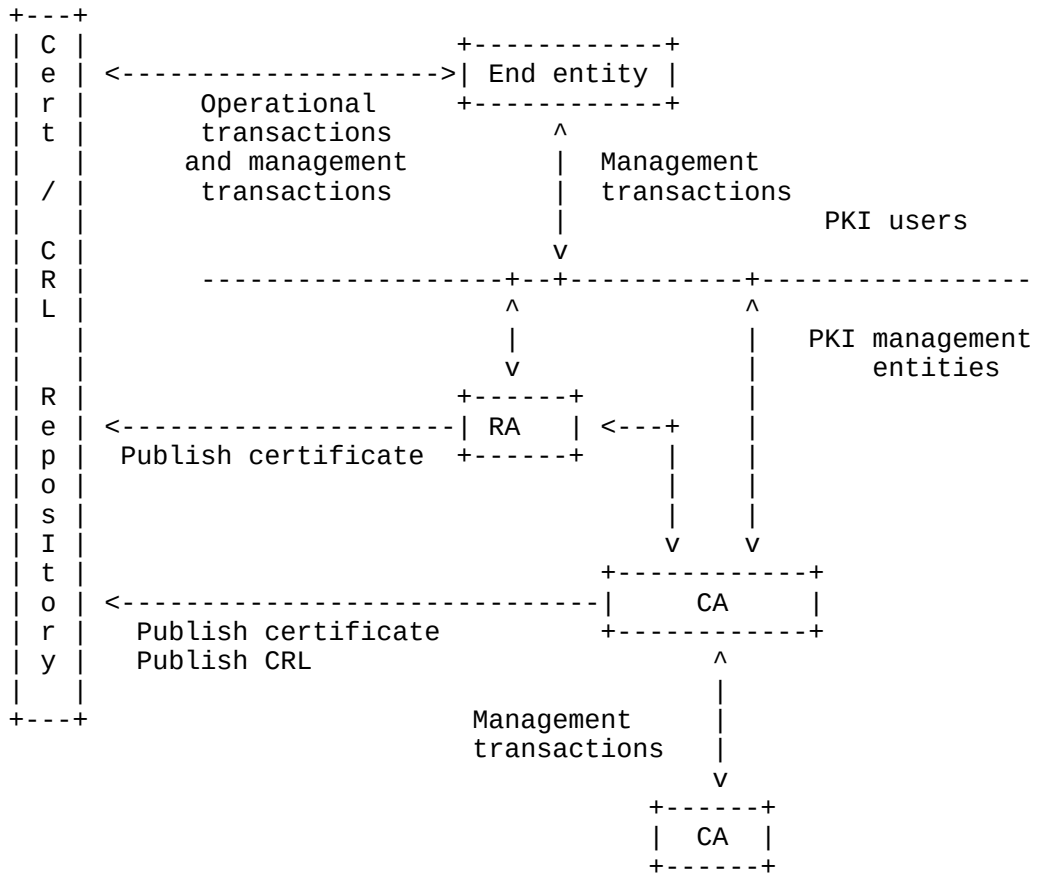
The protocol conventions described in this document satisfy some of the operational requirements of the Internet Public Key Infrastructure (PKI). This document specifies the conventions for using the File Transfer Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) to obtain certificates and certificate revocation lists (CRLs) from PKI repositories. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.

1 Introduction

This specification is part of a multi-part standard for the Internet Public Key Infrastructure (PKI) using X.509 certificates and certificate revocation lists (CRLs). This document specifies the conventions for using the File Transfer Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) to obtain certificates and CRLs from PKI repositories. Additional mechanisms addressing PKI repository access are specified in separate documents.

1.1. Model

The following is a simplified view of the architectural model assumed by the Internet PKI specifications.



The components in this model are:

End Entity: user of PKI certificates and/or end user system that is the subject of a certificate;

CA: certification authority;

RA: registration authority, i.e., an optional system to which a CA delegates certain management functions;

Repository: a system or collection of distributed systems that store certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

1.2. Certificate and CRL Repository

Some CAs mandate the use of on-line validation services, while others distribute CRLs to allow certificate users to perform certificate validation themselves. In general, CAs make CRLs available to certificate users by publishing them in the Directory. The Directory is also the normal distribution mechanism for certificates. However, Directory Services are not available in many parts of the Internet today. The File Transfer Protocol (FTP) defined in RFC 959 and the Hypertext Transfer Protocol (HTTP) defined in RFC 2068 offer alternate methods for certificate and CRL distribution.

End entities and CAs may retrieve certificates and CRLs from the repository using FTP or HTTP. End entities may publish their own certificate in the repository using FTP or HTTP, and RAs and CAs may publish certificates and CRLs in the repository using FTP or HTTP.

2 FTP Conventions

Within certificate extensions and CRL extensions, the URI form of GeneralName is used to specify the location where issuer certificates and CRLs may be obtained. For instance, a URI identifying the subject of a certificate may be carried in subjectAltName certificate extension. An IA5String describes the use of anonymous FTP to fetch certificate or CRL information. For example:

```
ftp://ftp.netcom.com/sp/spyrus/housley.cer
ftp://ftp.your.org/pki/id48.cer
ftp://ftp.your.org/pki/id48.no42.crl
```

Internet users may publish the URI reference to a file that contains their certificate on their business card. This practice is useful when there is no Directory entry for that user. FTP is widely deployed, and anonymous FTP are accommodated by many firewalls. Thus, FTP is an attractive alternative to Directory access protocols for certificate and CRL distribution. While this service satisfies the requirement to retrieve information related to a certificate which is already identified by a URI, it is not intended to satisfy the more general problem of finding a certificate for a user about whom some other information, such as their electronic mail address or corporate affiliation, is known.

For convenience, the names of files that contain certificates should have a suffix of ".cer". Each ".cer" file contains exactly one certificate, encoded in DER format. Likewise, the names of files that contain CRLs should have a suffix of ".crl". Each ".crl" file contains exactly one CRL, encoded in DER format.

3 HTTP Conventions

Within certificate extensions and CRL extensions, the URI form of GeneralName is used to specify the location where issuer certificates and CRLs may be obtained. For instance, a URI identifying the subject of a certificate may be carried in subjectAltName certificate extension. An IA5String describes the use of HTTP to fetch certificate or CRL information. For example:

```
http://www.netcom.com/sp/spyrus/housley.cer
http://www.your.org/pki/id48.cer
http://www.your.org/pki/id48.no42.crl
```

Internet users may publish the URI reference to a file that contains their certificate on their business card. This practice is useful when there is no Directory entry for that user. HTTP is widely deployed, and HTTP is accommodated by many firewalls. Thus, HTTP is an attractive alternative to Directory access protocols for certificate and CRL distribution. While this service satisfies the requirement to retrieve information related to a certificate which is already identified by a URI, it is not intended to satisfy the more general problem of finding a certificate for a user about whom some other information, such as their electronic mail address or corporate affiliation, is known.

For convenience, the names of files that contain certificates should have a suffix of ".cer". Each ".cer" file contains exactly one certificate, encoded in DER format. Likewise, the names of files that contain CRLs should have a suffix of ".crl". Each ".crl" file contains exactly one CRL, encoded in DER format.

4 MIME registrations

Two MIME types are defined to support the transfer of certificates and CRLs. They are:

```
application/pkix-cert
application/pkix-crl
```

4.1. application/pkix-cert

To: ietf-types@iana.org
Subject: Registration of MIME media type application/pkix-cert

MIME media type name: application

MIME subtype name: pkix-cert

Required parameters: None

Optional parameters: version (default value is "1")

Encoding considerations: will be none for 8-bit transports and most likely Base64 for SMTP or other 7-bit transports

Security considerations: Carries a cryptographic certificate

Interoperability considerations: None

Published specification: draft-ietf-pkix-ipki-part1

Applications which use this media type: Any MIME-complaint transport

Additional information:
Magic number(s): None
File extension(s): .CER
Macintosh File Type Code(s): none

Person & email address to contact for further information:
Russ Housley <housley@spyrus.com>

Intended usage: COMMON

Author/Change controller:
Russ Housley <housley@spyrus.com>

4.2. application/pkix-crl

To: ietf-types@iana.org
Subject: Registration of MIME media type application/pkix-crl

MIME media type name: application

MIME subtype name: pkix-crl

Required parameters: None

Optional parameters: version (default value is "1")

Encoding considerations: will be none for 8-bit transports and most likely Base64 for SMTP or other 7-bit transports

Security considerations: Carries a cryptographic certificate revocation list

Interoperability considerations: None

Published specification: draft-ietf-pkix-ipki-part1

Applications which use this media type: Any MIME-complaint transport

Additional information:
Magic number(s): None
File extension(s): .CRL
Macintosh File Type Code(s): none

Person & email address to contact for further information:
Russ Housley <housley@spyrus.com>

Intended usage: COMMON

Author/Change controller:
Russ Housley <housley@spyrus.com>

References

[RFC 959] Postel, J. and J. Reynolds, "File Transfer Protocol (FTP)", STD 5, RFC 959, October 1985.

[RFC 1738] Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[RFC 2068] Fielding, R., Gettys, J., Mogul, J., Frystyk, H. and T. Berners-Lee; "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, January 1997.

Security Considerations

Since certificates and CRLs are digitally signed, no additional integrity service is necessary. Neither certificates nor CRLs need be kept secret, and anonymous access to certificates and CRLs is generally acceptable. Thus, no privacy service is necessary.

HTTP caching proxies are common on the Internet, and some proxies do not check for the latest version of an object correctly. If an HTTP request for a certificate or CRL goes through a misconfigured or otherwise broken proxy, the proxy may return an out-of-date response.

Operators of FTP sites and World Wide Web servers should authenticate end entities who publish certificates as well as CAs and RAs who publish certificates and CRLs. However, authentication is not necessary to retrieve certificates and CRLs.

Authors' Addresses

Russell Housley
SPYRUS
381 Elden Street, Suite 1120
Herndon, VA 20170 USA

EMail: housley@spyrus.com

Paul Hoffman
Internet Mail Consortium
127 Segre Place
Santa Cruz, CA 95060 USA

EMail: phoffman@imc.org

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.