Network Working Group
Request for Comments: 4386
Category: Experimental

S. Boeyen
Entrust Inc.
P. Hallam-Baker
VeriSign Inc.

February 2006

Internet X.509 Public Key Infrastructure Repository Locator Service

Status of This Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document defines a Public Key Infrastructure (PKI) repository locator service. The service makes use of DNS SRV records defined in accordance with RFC 2782. The service enables certificate-using systems to locate PKI repositories.

Table of Contents

1. Overview

A number of RFCs (including [RFC2559], [RFC2560], and [RFC2585]) have specified operational protocols for retrieval of PKI data, including public-key certificates and revocation information, from PKI repositories. These RFCs assume that a certificate-using system has the information necessary to identify, locate, and connect to the PKI repository with a specific protocol. Although some tools are available in protocol-specific environments for this purpose, such as knowledge references in directory systems, these are restricted for use with a single protocol and do not share a common means of publication. This document provides a solution to this problem through the use of Service Record (SRV) Resource Records (RRs) in DNS. This solution is expected to be particularly useful in environments where only a domain name is available. In other situations (e.g., where a certificate is available that contains the required information), such a DNS lookup is not needed.

[RFC2782] defines a DNS RR for specifying the location of services (SRV). This document defines SRV records for a PKI repository locator service to enable PKI clients to obtain the necessary information to connect to a domain's PKI repository, including information about each protocol that is supported by that domain for access to its repository. This document includes the definition of an SRV RR format for this service and an example of its potential use in an email environment.

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in [RFC2119].

In examples, "C:" and "S:" indicate lines sent by the client and server, respectively.

2. SRV RR Definition

The format of the SRV RR, whose DNS type code is 33, is:

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

For the PKI repository locator service, this document uses the symbolic name "PKIXREP". Note that when used in an SRV RR, this name MUST be prepended with an "_" character.

The protocols that can be included in PKIXREP SRV RRs are:

Protocol	SRV Prefix
LDAP	_LDAP
HTTP	_HTTP
OCSP	_OCSP

2.1. Assignment of New Protocol Prefixes

Protocol prefix assignments for new PKIX repository protocols SHOULD be defined in the document that specifies the protocol.

2.2. Use of Multiple Repositories

The existence of multiple repositories MAY be determined by making separate DNS queries for each of the protocols supported by the client.

If this approach is found to be unacceptably inefficient due to a proliferation of repository protocols at a future date, the service discovery protocol could be extended to allow the repository to advertise the protocols supported.

2.3. SRV RR Example

This example uses the fictional domain "example.com" as an aid in understanding the use of SRV records by a certificate-using system.

Assume that Alice is an email client that needs a certificate for a recipient. Alice’s client system supports LDAP for certificate retrieval. Assume the message recipient is Bob and that Bob’s email address is bob@example.com. Assume that example.test maintains a "border directory" PKI repository and that Bob’s certificate is available from that directory, "border.example.com", via LDAP.

Alice’s client system retrieves, via DNS, the SRV record for _PKIXREP._LDAP.example.com.

- The QNAME of the DNS query is _PKIXREP._LDAP.example.com.
- The QCLASS of the DNS query is IN.
- The QTYPE of the DNS query is SRV.

The result SHOULD include the host address for example.com’s border directory system.

Note that if example.com operated its service on a number of hosts, more than one SRV RR would be returned. In this case, RFC 2782 defines the procedure to be followed in determining which of these should be accessed first.

3. Security Considerations

Security issues regarding PKI repositories themselves are outside the scope of this document. For LDAP repositories, for example, specific security considerations are addressed in RFC 2559.

Security issues with respect to the use of SRV records in general are addressed in RFC 2782, and these issues apply to the use of SRV records in the context of the PKIXREP service defined here.

4. IANA Considerations

This document reserves the use of "_PKIXREP" service label. Since this relates to a service that may pass messages over a number of different message transports, each message must be associated with a specific transport.

In order to ensure that the association between "_PKIXREP" and their respective underlying services is deterministic, the IANA has created a new registry: PKIX SRV Protocol Labels.

For this registry, an entry shall consist of a label name and a pointer to a specification describing how the protocol named in the label uses SRV. Specifications should conform to the requirements listed in [RFC2434] for "specification required".

5. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2559] Boeyen, S., Howes, T., and P. Richard, "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2", RFC 2559, April 1999.

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

Authors' Addresses

Sharon Boeyen
Entrust
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7

EMail: sharon.boeyen@entrust.com

Phillip M. Hallam-Baker
VeriSign Inc.
401 Edgewater Place, Suite 280
Wakefield MA 01880

EMail: pbaker@VeriSign.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).