Internet Draft
PKIX Working Group
July 2000
Expires in January 2001

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

Internet X.509 Public Key Infrastructure Repository Locator Service

<draft-ietf-pkix-pkixrep-00.txt>

1 Status of this Memo

1.1 Copyright Notice

2 Abstract

This document defines a 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 based on a domain name, identify the protocols that can be used to access the repository, and obtain addresses for the servers that host the repository service.

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].

3 Overview

Operational protocols have been specified for retrieval of PKI data, including public-key certificates and revocation information, from PKI repositories in a number of RFCs including RFC 2559, RFC 2560

---

and RFC 2585. These RFCs assume that a certificate using system has the knowledge information necessary to identify, locate and connect to the PKI repository with a specific protocol. Although there are some tools available in protocol-specific environments for this purpose, such as knowledge references in directory systems, these are restricted to use with a single protocol and do not share a common means of publication. This draft provides a solution to this problem through the use of SRV 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.

RFC 2782 defines a DNS RR for specifying the location of services (SRV). This Internet-draft 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 Internet-draft includes the defininition of a SRV RR format for this service and an example of its potential use in an email environment.

4 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 draft uses the symbolic name "PKIXREP". Note that when used in an SRV RR, this name MUST be prepended with a "_" character.

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

Note that when these protocol names appear in SRV records, they

MUST be prepended by a "_" character.

Other protocols could be added in future.

System administrators SHOULD create at least one PKIXREP SRV RR for each protocol that can be used to access their service. If the service is operated on a number of hosts, additional records can be created, as described in RFC 2782.

4.1 SRV RR example

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

Let an email client that needs a certificate for a recipient be Alice and assume that Alice's client system supports LDAP for certificate retrieval. Let the message recipient be Bob and let Bob's email address be bob@example.test. Assume that example.test maintains a "border directory" PKI repository and that Bob's

---

certificate is available from that directory "border.example.test" via LDAP.

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

- the QNAME of the DNS query is _PKIXREP._LDAP.example.test
- 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.test's border directory system.

Note that if example.test operated their 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.

5 Security considerations

Security issues regarding PKI repositories themselves are outside the scope of this specification. 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.

6 References

RFC 2119: Keywords for use in RFCs to indicate requirement levels.

RFC 2782: A DNS RR for specifying the location of services (DNS SRV)

RFC 2559: Internet X.509 Public Key Infrastructure
Operational Protocols - LDAPv2

RFC 2560: Internet X.509 Public Key Infrastructure
Online Certificate Status Protocol - OCSP

RFC 2585: Internet X.509 Public Key Infrastructure
Operational Protocols: FTP and HTTP

7 Authors' Addresses

Sharon Boeyen
Entrust Technologies
750 Heron Road, Suite 0800
Ottawa, Ontario
Canada K1V 1A7
email: sharon.boeyen@entrust.com

Phillip M. Hallam-Baker
VeriSign Inc.
401 Edgewater Place, Suite 280
Wakefield MA 01880
email: pbaker@VeriSign.com