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.
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.

Table of Contents

1. Overview.......................................................2
2. SRV RR definition..............................................2
   2.1 Assignment of new protocol prefixes..................3
   2.2 Use of multiple repositories........................3
   2.3 SRV RR example..........................................3
3. Security considerations........................................4
4. IANA Considerations............................................4
Copyright........................................................4
References........................................................5
Author’s Addresses................................................5

1. 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 definition of a SRV RR format for this service and an example of its potential use in an email environment.

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 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:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>SRV Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>_LDAP</td>
</tr>
<tr>
<td>HTTP</td>
<td>_HTTP</td>
</tr>
<tr>
<td>OCSP</td>
<td>_OCSP</td>
</tr>
</tbody>
</table>

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 fictional domain "example.com" 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.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 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.

3. 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.

4. IANA Considerations

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

In order to ensure that the association between "_PKIXREP" and their respective underlying services is deterministic, this document requests that IANA create a registry: The PKIX SRV Protocol Label.

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 RFC 2434 for "specification required".

Copyright

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights."

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE
References

[RFC 2119] Bradner, S., "Keywords for use in RFCs to indicate requirement levels, March 1997.


Author’s Addresses

Sharon Boeyen
Entrust
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
e-mail: sharon.boeyen@entrust.com

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