Internet Engineering Task Force
Internet-Draft
July 9, 2001

Ed Lewis
NAI Labs
Expires: January 9, 2002

DNS KEY Resource Record Generic Protocol Value
<draft-lewis-dnsext-key-genprot-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

This draft expires on January 9, 2002.

Abstract

A new protocol value is defined for the KEY Resource Record which identifies the intended protocol as that identified in the SRV-like encoding of the KEY RR's owner name.

1.0 Introduction

Starting with discussions concerning the mixing of zone keys and application keys at a zone apex, with the implication that the signing of the apex set makes the parent responsible for signing data inherently specific to the child zone, various proposals have been made to eliminate that issue. One such proposal is to separate keys by using the owner name, a la the SRV record. E.g., for a host named "host.myzone.test." a key used for SSH might be found at "_ssh._tcp.host.myzone.test." [RFC 2782]

Other motivations for this proposal and approach to naming key is to address issues including: concerns over size of the apex key set and

the extensive use of sub-typing KEY records. Since it is desirable to send the apex key set as additional data, it would be good to limit its size (by not having to include non-zone keys). Subtyping refers to making a resolver filter a returned RR set to extract the subset of records that meets the query's intent.

This draft is not intended to document the SRV naming proposal, nor are any of the examples represented here suggestions for naming conventions. The intent of the draft is to define a catch-all protocol value which informs a resolver that the intended protocol for this key is encoded in the ownership name.

If this (or a) generic protocol proposal is not adopted, yet a naming convention is used, the impact is that for each new protocol a new IANA-defined value is needed for the protocol octet in addition to a new specific naming convention. This proposal is just a means to ease the burden on IANA.

2.0 KEY RR Protocol Value

The unsigned integer value of <foobar> is reserved to mean that the owner name indicates the intended protocol of the KEY RR.

3.0 Acknowledgements

This proposal has been made in conversation with Jakob Schylter and Ilja Hallberg at a DNS meeting in Malmo Sweden.

4.0 IANA Considerations

A protocol number assignment for the DNS Key Resource Record is requested. The specific value is not considered important.

A suggestion to IANA is made regarding the KEY RR protocol values. One suggested assignment algorithm (perhaps this needs a different draft) is to assign the protocol number according to the reserved port number. This may help in uniqueness.

5.0 Security Considerations

This draft introduces no new security issues.

6.0 References

The text of any RFC may be retrieved by a web browser by requesting the URL: ftp://ftp.isi.edu/in-notes/rfc<wxyz>.txt, where "wxyz" is the number of the RFC.

[RFC 2026] "The Internet Standards Process -- Revision 3", Bradner
[RFC 2535] "Domain Name System Security Extensions", Eastlake
[RFC 2782] "A DNS RR for specifying the location of services (DNS SRV)", Gulbrandsen, Vixie, Esibov

7.0 Editor's Address

Edward Lewis
<lewis@tislabs.com>
3060 Washington Rd (Rte 97)
Glenwood, MD 21738
+1(443)259-2352

8.0 Full Copyright Statement