DNSEXT J. Reid
Internet-Draft Telnic Ltd
Expires: May 15, 2008 J. Schlyter
Kirei AB
B. Timms
Telnic Ltd
November 12, 2007

The NKEY DNS Resource Record
<draft-reid-dnsext-nkey-00.txt>

Status of this Memo

Copyright Notice

Abstract

A DNS Resource record which can be used to encrypt NAPTR records is described in this document.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC2119 [12].

2. Introduction

The DNS protocol is defined in RFC1034[1], RFC1035[2] and clarified in RFC2181[3]. The scope for using DNS KEY Resource Records was limited in RFC3445[4] to keys used by the Domain Name System Security Extensions (DNSSEC) which is defined in RFC4033[5], RFC4034[6] And RFC4035[7]. The original KEY RR used sub-typing to store both DNSSEC keys and arbitrary application keys. Storing both DNSSEC and application keys with the same record type is a mistake so RFC3445 removed application keys from the KEY record by redefining the Protocol Octet field in the KEY RR Data. This means that any other uses of keying material in the DNS need to define a new RRtype and mnemonic.

This document advocates the introduction of a new resource record specifically to provide this type of information for keys that encrypt NAPTR records [8]. A scheme for encrypting NAPTR records is outlined in draft-timms-encrypt-naptr [9].

3. Definition of NKEY Resource Record

The NKEY RR uses an IANA-assigned type code and is used as resource record for storing keys which encrypt NAPTR records. The RDATA for a NKEY RR consists of flags, a protocol octet, the algorithm number octet, and the public key itself. The format is as follows:

NKEY RDATA format

```
                   1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              flags            |   protocol    |   algorithm   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               /
   /                        public key                             /
   /                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

All bits of the flags field are reserved and MUST be zero. The protocol field MUST be set to 1. The algorithm and public key fields are identical to the definitions used in RFC4034 [6].

4. Security Considerations

The format and correct usage of DNSSEC keys is not changed by this document and no new security considerations are introduced.

5. IANA Considerations

IANA is requested to issue a new type code and mnemonic for the proposed resource record. No other IANA services are required by this document.

6. Acknowledgements

The authors would like to thank Klaus Malorny, Lawrence Conroy and Roy Arends for their constructive suggestions to this document and for helping to identify potential uses for the proposed record type.

7. References

7.1. Normative References

[1] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", RFC 1034, November 1987.

[2] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[3] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[4] Massey, D. and S. Rose, "Limiting the Scope of the KEY Resource Record (RR)", RFC 3445, December 2002.

[5] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[6] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[7] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[8] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[9] Timms, B., Reid, J., and J. Schlyter, "IANA Registration for Encrypted ENUM", draft-timms-enum-encrypt-00 (work in progress), November 2007.

[10] Braden, R., "Requirements for Internet Hosts -- Application and Support", RFC 1123, October 1989.

[11] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

7.2. Informative References

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

[13] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.

[14] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

[15] Bradner, S., "The Internet Standards Process -- Revision 3", RFC 2026, BCP 9, October 1996.

[16] Bradner, S., "IETF Rights in Contributions", BCP 78, RFC 3978, March 2005.

[17] Bradner, S., "Intellectual Property Rights in IETF Technology", BCP 79, RFC 3979, March 2005.

Authors' Addresses

Jim Reid
Telnic Ltd
6 Langside Court
Bothwell, SCOTLAND
United Kingdom

Phone: +44 20 7282 0000
Email: jim@telnic.org

Jakob Schlyter
Kirei AB
PO Box 53204
Goteborg, SE 40016
Sweden

Phone: +46 31 787 8007
Email: jakob@kirei.se

Ben Timms
Telnic Ltd
8 Wilfred Street
London, SW1T 6PL
United Kingdom

Phone: +44 20 7282 0000
Email: btimms@telnic.org

Full Copyright Statement

Intellectual Property

Acknowledgment

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