

DNS Extensions Working Group
Internet-Draft
Updates: RFC [2535](#), RFC TCR (if approved)
Expires: November 8, 2004

J. Schlyter, Ed.
May 10, 2004

DNSSEC NSEC RDATA Format
draft-ietf-dnsext-nsec-rdata-06.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/lid-abstracts.txt>.

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

This Internet-Draft will expire on November 8, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document redefines the wire format of the "Type Bit Map" field in the NSEC resource record RDATA format to cover the full RR type space.

Table of Contents

1.	Introduction	3
2.	The NSEC Resource Record	3
2.1	NSEC RDATA Wire Format	4
2.1.1	The Next Domain Name Field	4
2.1.2	The List of Type Bit Map(s) Field	4
2.1.3	Inclusion of Wildcard Names in NSEC RDATA	5
2.2	The NSEC RR Presentation Format	5
2.3	NSEC RR Example	5
3.	IANA Considerations	6
4.	Security Considerations	6
	Normative References	6
	Informational References	7
	Author's Address	7
A.	Acknowledgements	7
	Intellectual Property and Copyright Statements	8

1. Introduction

The NSEC [\[5\]](#) Resource Record (RR) is used for authenticated proof of the non-existence of DNS owner names and types. The NSEC RR is based on the NXT RR as described in [RFC 2535 \[2\]](#), and is similar except for the name and typecode. The RDATA format for the NXT RR has the limitation in that the RDATA could only carry information about the existence of the first 127 types. [RFC 2535](#) did reserve a bit to specify an extension mechanism, but the mechanism was never actually defined.

In order to avoid the need to develop an extension mechanism into a deployed base of DNSSEC aware servers and resolvers once the first 127 type codes are allocated, this document redefines the wire format of the "Type Bit Map" field in the NSEC RDATA to cover the full RR type space.

This document introduces a new format for the type bit map. The properties of the type bit map format are that it can cover the full possible range of typecodes, that it is relatively economical in the amount of space it uses for the common case of a few types with an owner name, that it can represent owner names with all possible types present in packets of approximately 8.5 kilobytes and that the representation is simple to implement. Efficient searching of the type bitmap for the presence of certain types is not a requirement.

For convenience and completeness this document presents the syntax and semantics for the NSEC RR based on the specification in [RFC 2535 \[2\]](#) and as updated by RFC TCR [\[5\]](#), thereby not introducing changes except for the syntax of the type bit map.

This document updates [RFC 2535 \[2\]](#) and RFC TCR [\[5\]](#).

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 [RFC 2119 \[1\]](#).

[2.](#) The NSEC Resource Record

The NSEC resource record lists two separate things: the owner name of the next RRset in the canonical ordering of the zone, and the set of RR types present at the NSEC RR's owner name. The complete set of NSEC RRs in a zone both indicate which RRsets exist in a zone and also form a chain of owner names in the zone. This information is used to provide authenticated denial of existence for DNS data, as described in [RFC 2535](#) [2].

The type value for the NSEC RR is 47.

Schlyter

Expires November 8, 2004

[Page 3]

Internet-Draft

DNSSEC NSEC RDATA Format

May 2004

The NSEC RR RDATA format is class independent and defined for all classes.

The NSEC RR SHOULD have the same TTL value as the SOA minimum TTL field. This is in the spirit of negative caching [8].

[2.1](#) NSEC RDATA Wire Format

The RDATA of the NSEC RR is as shown below:

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                               Next Domain Name                               /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                               List of Type Bit Map(s)                        /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

[2.1.1](#) The Next Domain Name Field

The Next Domain Name field contains the owner name of the next RR in the canonical ordering of the zone. The value of the Next Domain Name field in the last NSEC record in the zone is the name of the zone apex (the owner name of the zone's SOA RR).

A sender MUST NOT use DNS name compression on the Next Domain Name field when transmitting an NSEC RR.

Owner names of RRsets not authoritative for the given zone (such as glue records) MUST NOT be listed in the Next Domain Name unless at least one authoritative RRset exists at the same owner name.

[2.1.2](#) The List of Type Bit Map(s) Field

The RR type space is split into 256 window blocks, each representing the low-order 8 bits of the 16-bit RR type space. Each block that has at least one active RR type is encoded using a single octet window number (from 0 to 255), a single octet bitmap length (from 1 to 32) indicating the number of octets used for the window block's bitmap, and up to 32 octets (256 bits) of bitmap.

Window blocks are present in the NSEC RR RDATA in increasing numerical order.

"|" denotes concatenation

Type Bit Map(s) Field = (Window Block # | Bitmap Length | Bitmap) +

Each bitmap encodes the low-order 8 bits of RR types within the window block, in network bit order. The first bit is bit 0. For window block 0, bit 1 corresponds to RR type 1 (A), bit 2 corresponds to RR type 2 (NS), and so forth. For window block 1, bit 1 corresponds to RR type 257, bit 2 to RR type 258. If a bit is set to 1, it indicates that an RRset of that type is present for the NSEC RR's owner name. If a bit is set to 0, it indicates that no RRset of that type is present for the NSEC RR's owner name.

Since bit 0 in window block 0 refers to the non-existing RR type 0, it MUST be set to 0. After verification, the validator MUST ignore the value of bit 0 in window block 0.

Bits representing Meta-TYPES or QTYPES as specified in [RFC 2929](#) [3] ([section 3.1](#)) or within the range reserved for assignment only to QTYPES and Meta-TYPES MUST be set to 0, since they do not appear in zone data. If encountered, they must be ignored upon reading.

Blocks with no types present MUST NOT be included. Trailing zero octets in the bitmap MUST be omitted. The length of each block's bitmap is determined by the type code with the largest numerical value, within that block, among the set of RR types present at the

NSEC RR's owner name. Trailing zero octets not specified MUST be interpreted as zero octets.

[2.1.3](#) Inclusion of Wildcard Names in NSEC RDATA

If a wildcard owner name appears in a zone, the wildcard label ("*") is treated as a literal symbol and is treated the same as any other owner name for purposes of generating NSEC RRs. Wildcard owner names appear in the Next Domain Name field without any wildcard expansion. [RFC 2535](#) [2] describes the impact of wildcards on authenticated denial of existence.

[2.2](#) The NSEC RR Presentation Format

The presentation format of the RDATA portion is as follows:

The Next Domain Name field is represented as a domain name.

The List of Type Bit Map(s) Field is represented as a sequence of RR type mnemonics. When the mnemonic is not known, the TYPE representation as described in [RFC 3597](#) [4] ([section 5](#)) MUST be used.

[2.3](#) NSEC RR Example

The following NSEC RR identifies the RRsets associated with alfa.example.com. and identifies the next authoritative name after

Schlyter Expires November 8, 2004 [Page 5]

Internet-Draft DNSSEC NSEC RDATA Format May 2004

alfa.example.com.

alfa.example.com. 86400 IN NSEC host.example.com. A MX RRSIG NSEC TYPE1234

The first four text fields specify the name, TTL, Class, and RR type (NSEC). The entry host.example.com. is the next authoritative name after alfa.example.com. in canonical order. The A, MX, RRSIG, NSEC and TYPE1234 mnemonics indicate there are A, MX, RRSIG, NSEC and TYPE1234 RRsets associated with the name alfa.example.com.

The RDATA section of the NSEC RR above would be encoded as:

```
0x04 'h' 'o' 's' 't'
0x07 'e' 'x' 'a' 'm' 'p' 'l' 'e'
0x03 'c' 'o' 'm' 0x00
```

```
0x00 0x06 0x40 0x01 0x00 0x00 0x00 0x03
0x04 0x1b 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x20
```

Assuming that the resolver can authenticate this NSEC record, it could be used to prove that beta.example.com does not exist, or could be used to prove there is no AAAA record associated with alfa.example.com. Authenticated denial of existence is discussed in [RFC 2535](#) [2].

3. IANA Considerations

This document introduces no new IANA considerations, because all of the protocol parameters used in this document have already been assigned by RFC TCR [5].

4. Security Considerations

The update of the RDATA format and encoding does not affect the security of the use of NSEC RRs.

Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Eastlake, D., "Domain Name System Security Extensions", [RFC 2535](#), March 1999.
- [3] Eastlake, D., Brunner-Williams, E. and B. Manning, "Domain Name System (DNS) IANA Considerations", [BCP 42](#), [RFC 2929](#), September

Schlyter	Expires November 8, 2004	[Page 6]
----------	--------------------------	----------

Internet-Draft	DNSSEC NSEC RDATA Format	May 2004
----------------	--------------------------	----------

2000.

- [4] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", [RFC 3597](#), September 2003.
- [5] Weiler, S., "Legacy Resolver Compatibility for Delegation Signer", [draft-ietf-dnsext-dnssec-2535typecode-change-05](#) (work in progress), October 2003.

Informational References

- [6] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), November 1987.
- [7] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [8] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", [RFC 2308](#), March 1998.

Author's Address

Jakob Schlyter (editor)
Karl Gustavsgatan 15
Goteborg SE-411 25
Sweden

E-Mail: jakob@schlyter.se

[Appendix A](#). Acknowledgements

The encoding described in this document was initially proposed by Mark Andrews. Other encodings were proposed by David Blacka and Michael Graff.

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the
Internet Society.

Schlyter

Expires November 8, 2004

[Page 9]