# Verifying Resource Records Without Knowing Their Contents

## Status of This Memo



## Abstract

DNSSEC [RFC2065] provides a mechanism to cryptographically verify a DNS resource record provided we can get it into canonical form.

The problem is how do we do this without knowing the contents of all resource record types?

This document provides one possible solution to this problem.

## 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 [RFC2119].

## 2 - Method

In order to be able to canonicalise a resource record a resolver needs to know where in the data domain names exist so that the resolver can decompress the domain names and convert the uppercase ASCII in ordinary labels to lowercase prior to the data being feed into the encryption routines.

This document propose that all new resource record types defined MUST have a header at the start of the data section locating where the domain names are in the data section. A new resource record for the purpose of this document is any type NOT referenced in section 3 Old Types. Meta queries such as MAILA (254), MAILB (253), AXFR (252) and IXFR (251) are not covered by this document as they do not return data of this type.

This table would be a series of unsigned 16 bit words in network order. The first word contains the length of the table as 16 bit words not counting the first word. Subsequent words contain the offset from the start of the data to the start of relevent domain name in the data assuming all domain names are uncompressed. Offsets in the table are in the same order as domain names in the data.

## 3 Old Types

The following types are deemed old and are NOT covered by this document. A (1), NS (2), MD (3), MF (4), CNAME (5), SOA (6), MB (7), MG (8), MR (9), NULL (10), WKS (11), PTR (12), HINFO (13), MINFO (14), MX (15), TXT (16), RP (17), AFSDB (18), X25 (19), ISDN (20), RT (21), NSAP (22), NSAP-PTR (23), SIG (24), KEY (25), PX (26), GPOS (27), AAAA (28), LOC (29), NXT (30), EID (31), NIMLOC (32), SRV (33), ATMA (34), NAPTR (35), KX (36), CERT (37), A6 (38), DNAME (39), UINFO (100), UID (101), GID (102), UNSPEC (103), OPT (XXX), TKEY (249) and TSIG (250).

## 4 Security Considerations

It is believed that this document does not introduce any significant additional security threats other that those that already exist when using data from the DNS but rather enhances security by allowing new resource record types to be checked by security aware resolvers.

## 5 IANA Considerations

This document places no requirements apon IANA.

## References

[RFC2065]
Eastlake, D. 3rd. and Kaufman, C,. "Domain Name System Security Extensions," RFC 2065, January 1997

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997

## Author's Address

Mark Andrews
Internet Software Consortium
1 Seymour St.
Dundas Valley
NSW 2117
AUSTRALIA
+61 2 9871 4742
<Mark_Andrews@isc.org>