Network Working Group
Request for Comments: 4431
Category: Informational

M. Andrews
Internet Systems Consortium
S. Weiler
SPARTA, Inc.

February 2006

The DNSSEC Lookaside Validation (DLV) DNS Resource Record

Status of This Memo

Copyright Notice

Abstract

This document defines a new DNS resource record, called the DNSSEC Lookaside Validation (DLV) RR, for publishing DNSSEC trust anchors outside of the DNS delegation chain.

1. Introduction

DNSSEC [1] [2] [3] authenticates DNS data by building public-key signature chains along the DNS delegation chain from a trust anchor, ideally a trust anchor for the DNS root.

This document defines a new resource record for publishing such trust anchors outside of the DNS's normal delegation chain. Use of these records by DNSSEC validators is outside the scope of this document, but it is expected that these records will help resolvers validate DNSSEC-signed data from zones whose ancestors either aren't signed or refuse to publish delegation signer (DS) records for their children.

2. DLV Resource Record

The DLV resource record has exactly the same wire and presentation formats as the DS resource record, defined in RFC 4034, Section 5. It uses the same IANA-assigned values in the algorithm and digest type fields as the DS record. (Those IANA registries are known as the "DNS Security Algorithm Numbers" and "DS RR Type Algorithm Numbers" registries.)

The DLV record is a normal DNS record type without any special processing requirements. In particular, the DLV record does not inherit any of the special processing or handling requirements of the DS record type (described in Section 3.1.4.1 of RFC 4035). Unlike the DS record, the DLV record may not appear on the parent's side of a zone cut. A DLV record may, however, appear at the apex of a zone.

3. Security Considerations

For authoritative servers and resolvers that do not attempt to use DLV RRs as part of DNSSEC validation, there are no particular security concerns -- DLV RRs are just like any other DNS data.

Software using DLV RRs as part of DNSSEC validation will almost certainly want to impose constraints on their use, but those constraints are best left to be described by the documents that more fully describe the particulars of how the records are used. At a minimum, it would be unwise to use the records without some sort of cryptographic authentication. More likely than not, DNSSEC itself will be used to authenticate the DLV RRs. Depending on how a DLV RR is used, failure to properly authenticate it could lead to significant additional security problems including failure to detect spoofed DNS data.

RFC 4034, Section 8, describes security considerations specific to the DS RR. Those considerations are equally applicable to DLV RRs. Of particular note, the key tag field is used to help select DNSKEY RRs efficiently, but it does not uniquely identify a single DNSKEY RR. It is possible for two distinct DNSKEY RRs to have the same owner name, the same algorithm type, and the same key tag. An implementation that uses only the key tag to select a DNSKEY RR might select the wrong public key in some circumstances.

For further discussion of the security implications of DNSSEC, see RFC 4033, RFC 4034, and RFC 4035.

4. IANA Considerations

IANA has assigned DNS type code 32769 to the DLV resource record from the Specification Required portion of the DNS Resource Record Type registry, as defined in [4].

The DLV resource record reuses the same algorithm and digest type registries already used for the DS resource record, currently known as the "DNS Security Algorithm Numbers" and "DS RR Type Algorithm Numbers" registries.

5. Normative References

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

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

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

[4] Eastlake, D., Brunner-Williams, E., and B. Manning, "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 2929, September 2000.

Authors' Addresses

Mark Andrews
Internet Systems Consortium
950 Charter St.
Redwood City, CA 94063
US

EMail: Mark_Andrews@isc.org

Samuel Weiler
SPARTA, Inc.
7075 Samuel Morse Drive
Columbia, Maryland 21046
US

EMail: weiler@tislabs.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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