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


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

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions
contained in BCP 78, and except as set forth therein, the authors
retain all their rights.

This document and the information contained herein are provided on an
"AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS
OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET
ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any
Intellectual Property Rights 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; nor does it represent that it has
made any independent effort to identify any such rights. Information
on the procedures with respect to rights in RFC documents can be
found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this
specification can be obtained from the IETF on-line IPR repository at

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights that may cover technology that may be required to implement
this standard. Please address the information to the IETF at
ietf-ipr@ietf.org.

Acknowledgement

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