Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: August 31, 2010

N. Kong
Y. Zhang
X. Lee
CNNIC

February 27, 2010

DNSSEC Lookaside Validation Trust Alliance (DLVTA) of Multiple DNSSEC Lookaside Validation (DLV) Domains
draft-kong-dnsop-dlv-trust-alliance-00

Abstract

This document describes a methodology for constructing DNSSEC Lookaside Validation Trust Alliance (DLVTA) of multiple DNSSEC Lookaside Validation (DLV) domains without disrupting the deployment of standard DNSSEC. The DLVTA allows validating resolvers to validate DNSSEC-signed data from multiple DLV domains without maintaining a series of trust anchors for those different DLV domains in their name server configurations.

Table of Contents

1. Introduction

DNSSEC [RFC4033] [RFC4034] [RFC4035] authenticates Domain Name System (DNS) data by building public-key signature chains along the DNS authentication chain from a trust anchor.

DNSSEC Lookaside Validation (DLV) [RFC4431] [RFC5074] allows the deployment of DNSSEC in the absence of a signed DNS tree at the root, Top Level Domain (TLD) and near-top levels. DLV provides an additional entry point from which to obtain the DNSSEC validation information.

DLV allows a set of DLV domains to publish secure entry points for zones that are not their own children as described in [RFC5074]. In future, there will be multiple DLV domains operated by different organizations for different zones whose ancestors either aren't signed or don't publish Delegation Signer (DS) records [RFC4034] for their children. For example, the DLV domain dlv.example.zone1 targets the zone1 zone, the DLV domain dlv.example.zone2 targets the zone2 zone, and the DLV domain dlv.example.zone3 targets the zone3 zone. "In the interest of limiting complexity, validators SHOULD NOT attempt to use DLV to validate data from another DLV domain.", as described in Section 5 of [RFC5074]. So Users wanting to make use of DNSSEC would need to know all of these DLV domains beforehand, and then need to maintain a series of trust anchors in their name server configurations, corresponding to the different DLV domains that publish the cryptographic keys they use to sign their zones. Discovering all of this DLV domains, and maintaining all related information up to date can turn into a tough task along with the increase of the number of the DLV domains in the future.

This document describes a methodology for constructing DNSSEC Lookaside Validation Trust Alliance (DLVTA) of multiple DNSSEC Lookaside Validation (DLV) domains without disrupting the deployment of standard DNSSEC. The DLVTA allows validating resolvers to validate DNSSEC-signed data from multiple DLV domains without maintaining a series of trust anchors for those different DLV domains in their name server configurations.

2. 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].

3. Architecture

DLVTA allows a set of DLVTA domains to publish trust anchors of DLV domains that are not their own children. Through a DLVTA domain, a validator may expect the named DLV domains to be trusted.

The structure of DLVTA is shown in Figure 1.

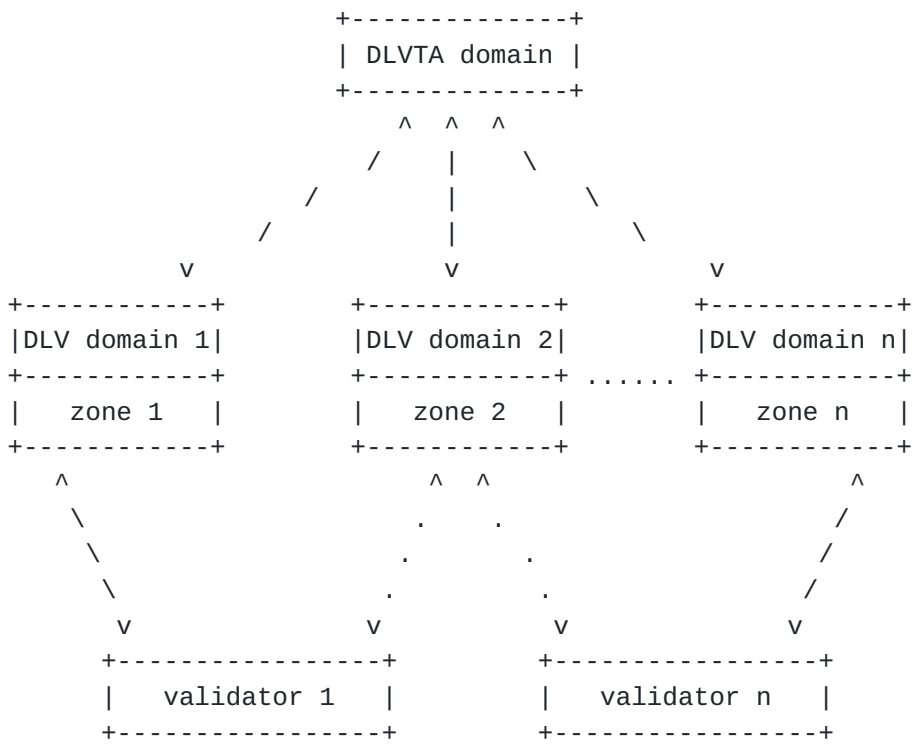

Figure 1

In the above figure, there are n zones (from zone 1 to zone n), and each one chooses its own DLV domains (from DLV domain 1 to DLV domain n). For example, the DLV domain 1 is used by the zone 1, and the DLV domain n is used by the zone n. All of these DLV domains is contained within a DLVTA Domain.

Without DLVTA, any validator which only sets one of these DLV domains (such as the DLV domain 1) as its sole trust anchor can only validate the DNSSEC-signed data from one zone (zone 1). But through DLVTA, any validator which sets a DLVTA domain as its trust anchor can discovery DLV domains within the DLVTA domain, and then obtain any DNSSEC validation information of zones by these DLV domains. For example, the validator 1 uses DLV domain 1 as its trust anchor, and the validator 2 uses DLV domain n as its trust anchor. If both of them set the DLVTA domain in figure 1 as their trust anchor, they can obtain the DNSSEC validation information of the zone 2 through DLVTA.

4. The DLVTA DNS Resource Record

The DLVTA DNS resource record can be divided into two kinds, DLVTA Target Information (DLVTATI) resource record and DLVTA Key Information (DLVTAKI) resource record. The first one is used to store the target information of DLV domains within a DLVTA domain, and the second one is used to store the public key information of DLV domains within a DLVTA domain.

4.1. DLVTATI Resource Record

The DLVTATI resource record has exactly the same wire and presentation formats as the NAPTR resource record, defined in [RFC2915].

The format of the DLVTATI resource record is given below.

Name TTL Class Type Order Preference Flags Service Regexp Replacement

- Name: The domain name to which this resource record refers. The Name field MUST be the named of the targeted zone by a DLV domain plus the name of the DLVTA domain.

- TTL: Standard DNS meaning [RFC1035].

- Class: Standard DNS meaning [RFC1035].

- Type: The Type Code [RFC1035] for DLVTATI is XX.

- Order: The Order field is not be used. It SHALL be set to zero.

- Preference: A 16-bit unsigned integer defined by [RFC2915]. Low numbers SHOULD be processed before high numbers.

- Flags: The Flags field MUST be set to 'u', indicating that the Regexp field contains a URI.

- Service: The Service field is not be used. It SHALL be set to the empty string.

- Regexp: The Regexp field specifies a DLV domain within the DLVTA domain. The value of this field SHOULD be the string !^.*$! (the six character sequence consisting of an exclamation point, a caret, a period, an asterisk, a dollar sign, and another exclamation point), followed by a URI, followed by an exclamation point (!) character.

- Replacement: The Replacement field is not be used. It SHOULD be set to a single period ('.').

For example, the DLV domain dlv1.example.zone1, the DLV domain dlv2.example.zone1, and the DLV domain dlv.example.zone2 belong to a DLVTA domain dlvta.example.zone3. The DLVTA domain dlvta.example.zone3 SHOULD have DLVTATI resource records to store the target information of the DLV domain dlv1.example.zone1, the DLV domain dlv2.example.zone1, and the DLV domain dlv.example.zone2.

Name TTL Class Type Order Preference Flags Service Regexp Replacement
zone1.dlvta.example.zone3. 86400 IN DLVTATI 0 10 "u" " "
"!^.*$!dlv1.example.zone1!" .

zone1.dlvta.example.zone3. 86400 IN DLVTATI 0 100 "u" " "
"!^.*$!dlv2.example.zone1!" .

zone2.dlvta.example.zone3. 86400 IN DLVTATI 0 10 "u" " "
"!^.*$!dlv.example.zone2!" .

In the example above, both the DLV domain dlv1.example.zone1 and DLV domain dlv2.example.zone1 target the zone1, but the DLV domain dlv1.example.zone1 should be used before the DLV domain dlv2.example.zone1 by validators because of the value of the Preference field.

4.2. DLVTAKI Resource Record

The DLVTAKI resource record has exactly the same wire and presentation formats as the DLV resource record, defined in [RFC4431]. It uses the same IANA-assigned values in the algorithm and digest type fields as the DS record.

Any DLVTA domain SHOULD store the public key information of DLV domains within the DLVTATI resource record by the DLVTAKI resource record.

The Name field MUST be the named of the DLV domain plus the name of the DLVTA domain.

For example, the DLV domain dlv.example.zone1 and the DLV domain dlv.example.zone2 belong to a DLVTA domain dlvta.example.zone3. The DLVTA domain dlvta.example.zone3 SHOULD has a DLVTAKI resource record to store the public key information of the DLV domain dlv.example.zone1 and the DLV domain dlv.example.zone2.

Name TTL Class TypeKey Tag Algorithm DigestType Digest
dlv.example.zone1.dlvta.example.zone3. 86400 IN DLVTAKI 29092 5 1 (

```
224 3B4148AAF0494943209B666DD5C5FC6B200CD )

dlv.example.zone2.dlvta.example.zone3. 86400 IN DLVTAKI 25081 5 1 (
D6C 409078DAAF3C4C5354161E71CA276819DC504 )
```

5. The Validator Behavior using DLVTA

A validator using DLVTA SHOULD first attempt validation using any applicable (non-DLV) trust anchors, and then DLV processing occurs only if the validation fails, as described in [RFC5074]. The DLVTA processing occurs only after the DLV validation fails, that is to say, if the DLV validation succeeds (with a result of Secure), DLVTA processing need not occur.

When DLVTA processing occurs, a validator looks for a closest enclosing DLVTATI RRset in the DLVTA domain, which is the DLVTATI RRset with the longest name that matches the query or could be an ancestor of the QNAME. To find the closest enclosing DLVTATI RRset for a given query, the validator starts by looking for a DLVTATI RRset corresponding to the QNAME. For example, assuming there exist DLVTATI RRsets named zone1.dlvta.example.zone, sub.zone1.dlvta.example.zone, example.sub.zone1.dlvta.example.zone within a DLVTA domain dlvta.example.zone. A validator would use the example.sub.zone1.dlvta.example.zone DLVTATI RRset for validating responses to a query for example.sub.zone1.

When a validator finds a closest enclosing DLVTATI RRset in the DLVTA domain, it would regard the URI inside the Regexp field of the DLVTATI RRset as a DLV domain which targets the zone named by the Name field (MUST remove the part of the DLVTA domain) of the DLVTATI RRset. And then it SHOULD use the DLVTAKI which has the same Name field with the name of the DLV domain plus the name of the DLVTA domain, as though it were a DS RRset to validate the answer of the DLV domain using the normal procedures in Section 5 of [RFC4035]. If the validation succeeds, the validator SHOULD attempt validation using the DLV domain as described in . [RFC5074].

It's possible that a DLV domain obtained from a DLVTA domain by a validator is a default trust anchor in its name server configurations. To avoid the repeat query for the DLV domain, the validator SHALL ignore it in the process of the DLVTA validation.

The flow of the validator behavior using DLVTA is shown in Figure 2.

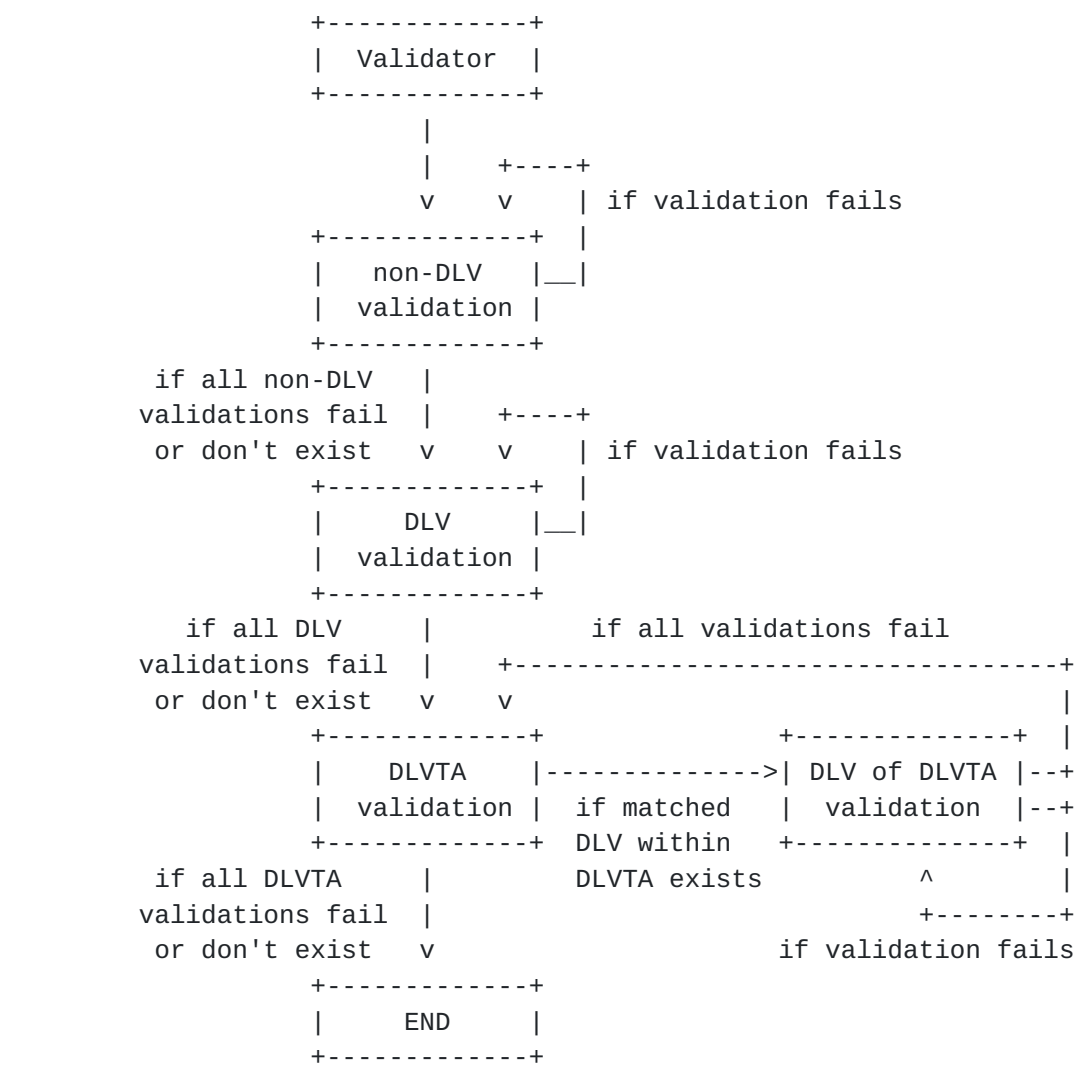

Figure 2

6. Examples

NOTE: These are examples only. They are taken from ongoing work and may not represent the end result of that work. They are here for pedagogical reasons only.

Assuming zone1, zone2 and zone3 aren't signed by its parent. The DLV domain dlv.example.zone1 targets the zone1 zone, the DLV domain dlv.example.zone2 targets the zone2 zone, and the DLV domain dlv.example.zone3 targets the zone3 zone. The DLVTA domain dlvta.example.zone1 contains the dlv.example.zone1 and the DLV domain dlv.example.zone2. The DLVTA domain dlvta.example.zone2 contains the dlv.example.zone1, DLV domain dlv.example.zone2 and the DLV domain dlv.example.zone3.

6.1. Example 1

Assuming the validator 1 uses the DLV domain dlv.example.zone1 as a default trust anchor of DLV, and uses the DLVTA domain dlvta.example.zone1 as a default trust anchor of DLVTA in its name server configurations.

- dnssec-lookaside "zone1" trust-anchor "dlv.example.zone1";

- dnssec-lookaside-trust-alliance trust-anchor "dlvta.example.zone1";

The validator 1 can validate DNSSEC-signed data from zone 1 by its default DLV (dlv.example.zone1), and it can get the appropriate DLV (dlv.example.zone2) for zone2 from its default DLVTA (dlvta.example.zone1). Then the validator 1 can validate DNSSEC-signed data from zone 2 by DLV (dlv.example.zone2).

6.2. Example 2

Assuming the validator 2 uses the DLV domain dlv.example.zone2 as a default trust anchor of DLV, and uses the DLVTA domain dlvta.example.zone2 as a default trust anchor of DLVTA in its name server configurations.

- dnssec-lookaside "zone2" trust-anchor "dlv.example.zone2";

- dnssec-lookaside-trust-alliance trust-anchor "dlvta.example.zone2";

The validator 2 can validate DNSSEC-signed data from zone 2 by its default DLV (dlv.example.zone2). It can get the appropriate DLV (dlv.example.zone1) for zone1, and DLV (dlv.example.zone3) for zone3 from its default DLVTA (dlvta.example.zone2). Then the validator 2 can validate DNSSEC-signed data from zone 1 by DLV (dlv.example.zone1), and validate DNSSEC-signed data from zone 3 by DLV (dlv.example.zone3).

7. IANA Considerations

IANA is requested to assignment the DNS type code XX to the DLVTATI resource record, and the DNS type code XX to the DLVTAKI resource record from the Specification Required portion of the DNS Resource Record Type registry, as defined in [RFC2929].

The DLVTAKI 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.

8. Security considerations

For authoritative servers and resolvers that do not attempt to use DLVTA RRs as part of DNSSEC validation, there are no particular security concerns.

Validators using DLVTA MUST NOT use a DLVTA record unless it has been successfully authenticated. Normally, validators will have a trust anchor for the DLVTA domain and use DNSSEC to validate the data in it.

For further discussion of the security implications of DNSSEC and DLV, see [RFC4033], [RFC4034], [RFC4035], [RFC4431], [RFC5074].

9. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

[RFC2915] Mealling, M. and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2915, September 2000.

[RFC2929] Eastlake, D., Brunner-Williams, E., and B. Manning, "Domain Name System (DNS) IANA Considerations", RFC 2929, September 2000.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4431] Andrews, M. and S. Weiler, "The DNSSEC Lookaside Validation (DLV) DNS Resource Record", RFC 4431,

February 2006.

[RFC5074] Weiler, S., "DNSSEC Lookaside Validation (DLV)", RFC 5074, November 2007.

Authors' Addresses

Ning Kong
CNNIC
4 South 4th Street,Zhongguancun,Haidian District
Beijing, Beijing 100190
China

Phone: +86 10 5881 3147
Email: nkong@cnnic.cn

Yuedong Zhang
CNNIC
4 South 4th Street,Zhongguancun,Haidian District
Beijing, Beijing 100190
China

Phone: +86 10 5881 2635
Email: zhangyuedong@cnnic.cn

Xiaodong Lee
CNNIC
4 South 4th Street,Zhongguancun,Haidian District
Beijing, Beijing 100190
China

Phone: +86 10 5881 3020
Email: lee@cnnic.cn