Internet Engineering Task Force S. Huque
Internet-Draft P. Aras
Intended status: Informational Salesforce
Expires: September 03, 2018 March 02, 2018

Multi Provider DNSSEC models
draft-huque-dnsop-multi-provider-dnssec-00

Abstract

Many enterprises today employ the service of multiple DNS providers to distribute their authoritative DNS service. Deploying DNSSEC in such an environment can have some challenges depending on the configuration and feature set in use. This document will present several deployment models that may be suitable.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 03, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and Motivation

Many enterprises today employ the service of multiple DNS providers to distribute their authoritative DNS service. Two providers are fairly typical and this allows the DNS service to survive a complete failure of any single provider. This document outlines some possible models of DNSSEC deployment in such an environment.

2. Deployment Models

The two main models discussed are (1) where the zone owner runs a master signing server and essentially treats the managed DNS providers as secondary servers, the "Serve Only" model, and (2) where the managed DNS providers each act like primary servers, signing data received from the zone owner and serving it out to DNS queriers, the "Sign and Serve" model.

2.1. Serve Only model

The most straightforward deployment model is one in which the zone owner runs a primary master DNS server, and manages the signing of zone data. The master server uses DNS zone transfer mechanisms (AXFR /IXFR) to distribute the signed zone to multiple DNS providers.

This is also arguably the most secure model because the zone owner holds the private signing keys. The managed DNS providers cannot serve bogus data (either maliciously or because of compromise of their systems) without detection by validating resolvers.

One notable limitation of this model is that it may not work with DNS authoritative server configurations that use certain non-standardized DNS features. Some of these features like DNS based Global Server Load Balancing (GSLB), dynamic failover pools, etc. rely on querier specific responses, or responses based on real-time state examination, and so, the answer and corresponding signature has to be determined at the authoritative server being queried, at the time of the query, or both.

2.2. Sign and Serve models

In this category of models, multiple providers each independently sign and serve the same zone. The zone owner typically uses provider-specific APIs to update zone content at each of the providers, and relies on the provider to perform signing of the data. The main challenge here is to manage the contents of the DNSKEY and DS RRset in such a way that validating resolvers always have a viable path to authenticate the DNSSEC signature chain no matter which provider they query and obtain responses from.

These models can support DNSSEC even for the non-standard features mentioned previously, if the DNS providers have the capability of signing the response data generated by those features. Since these responses are often generated dynamically at query time, one method is for the provider to perform online signing (also known as on-the-fly signing). However, another possible approach is to pre-compute all the possible response sets and associated signatures and then algorithmically determine at query time which response set needs to be returned.

In these models, the function of coordinating the DNSKEY or DS RRset does not involve the providers communicating directly with each other, which they are unlikely to do since they typically have a contractual relationship only with the customer.

The following descriptions consider the case of two DNS providers, but the model is generalizable to any number.

2.2.1. Model 1

- Customer holds the KSK and manages the DS record.
- Each provider has their own ZSK which is used to sign data
- Providers have an API that customer uses to query the ZSK public key, and insert a combined DNSKEY RRset that includes both ZSKs and the KSK, signed by the KSK.

- Key rollovers need coordinated customer participation to update and re-sign the DNSKEY RRset.

2.2.2. Model 2

- Each provider has their own KSK and ZSK.
- Each provider also includes the ZSK of the other provider - delivered to them by the customer via some API mechanism
- DNSKEY RRset is signed independently by each provider using their own KSK.
- Customer manages the DS record that includes both KSKs.
- KSK rollovers need coordinated customer participation to update the DS.

2.2.3. Model 3

Possible models in which KSK and/or ZSK key pairs are shared across providers are not currently discussed. Preliminary discussion with some providers has revealed that this is not a mode all of them are comfortable with, as they do not want to share signing keys with other parties.

2.3. Inline Signing models

In this model, the zone owner runs a master server but does not perform zone signing, instead pushing out the zone (typically via zone transfer mechanisms) to multiple providers, and relying on those providers to sign the zone data before serving them out. This model has to address the same set of requirements as the Sign-and-Serve model regarding managing the DNSKEY and DS RRsets. However, assuming standardized zone transfers mechanisms are being used to push out the zone to the providers, it likely also has the limitation that non-standardized DNS features cannot be supported or signed. This model is not discussed further.

3. Signing Algorithm Considerations

[TBD: at the very least we have to consider whether any or all of these schemes require algorithms to be the same or not, or benefit from algorithms being the same. Current DNS specifications indicate that if there are multiple algorithms in the DNSKEY RRset, then data records need to be signed with at least one of each algorithm, (how does that work with online signing?). Multiple signatures per record set is a cost that probably few operators want to bear.]

4. Validating Resolver Behavior

TBD

5. Key Rollover Considerations

TBD

6. IANA Considerations

This document includes no request to IANA.

7. Security Considerations

[TBD]

8. References

8.1. Normative References

[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.

8.2. Informative References

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

Authors' Addresses

Shumon Huque
Salesforce

Email: shuque@gmail.com

Pallavi Aras
Salesforce

Email: paras@salesforce.com