Internet Engineering Task Force
Internet-Draft
Updates: 4034, 4035 (if approved)
Intended status: Standards Track
Expires: 4 September 2025

M. Andrews
Internet Systems Consortium
S. Huque
Salesforce
Y. Thessalonikefs
NLnet Labs

3 March 2025

Collision Free Keytags for DNSSEC
draft-huque-dnsop-keytags-01

Abstract

DNSSEC employs a Key Tag field in the RRSIG and DS resource records in order to efficiently identify the key that produced a DNSSEC signature and the key that should be used as a secure entry point into a delegated zone. The Key Tag was not intended to be a unique identifier. Key tag collisions can occur in practice for keys in the same zone, though they are relatively rare in normal operation. Colliding key tags impose additional work on a validating resolver because it then has to check signatures for each of the candidate set of keys identified by the Key Tag. Furthermore, they open up resolvers to computational denial of service attacks by adversaries deploying specially crafted zones with many intentionally colliding key tags. This document specifies updates to the DNSSEC protocol and the process of key generation to avoid colliding key tags.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/shuque/ietf-dns-keytags.

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 https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

DNSSEC [RFC4033] [RFC4034] [RFC4035] employs a Key Tag field in the RRSIG and DS resource records in order to efficiently identify the key that produced a DNSSEC signature the key that should be used as secure entry point into a delegated zone. The Key Tag was not intended to be a unique identifier. Key tag collisions can occur in practice for keys in the same zone, though they are relatively rare in normal operation. Colliding key tags impose additional work on a validating resolver because it then has to check signatures for each of the candidate set of keys identified by the Key Tag. Furthermore, they open up resolvers to computational denial of service attacks by adversaries deploying specially crafted zones with many intentionally colliding key tags [KEYTRAP]. This document specifies updates to the DNSSEC protocol and the process of key generation to avoid colliding

key tags.

2. Protocol Behavior

* New DNSKEY algorithms MUST have DNSKEY RRsets that do not have colliding key tags

* What about existing algorithms? Should we have new aliases for existing algorithms that allow us to incorporate the non collision requirement?

* Can we propose a future flag date after which existing algorithms will be required to enforce this requirement?

* Outline the general process by which key generation software should ensure uniqueness of keytags.

* Special considerations for multi-signer [RFC8901] configurations, where multiple distinct parties generate their own keys for the same zone (i) partition the keytag space between each signer/ provider, and have each provider re-generate keys if necessary until they obtain one whose keytag is contained in their partition (ii) Use a central key broker to enforce keytag uniqueness, (iii) each signer when generating new keys, queries all DNSKEYs in the multi-signer group to avoid colliding keys. To avoid race conditions, ideally the providers should not generate keys at the same time, and plausibly the zone owner could enforce non-conflicting key generation schedules across the multi-signer group.

* Describe what to do when a validator encounters a zone with both old and new DNSKEY algorithm numbers.

* For possible discussion: recommend the use DNS cookies to avoid offpath computational DoS attacks.

3. Updates to RFCs

TBD

4. Security Considerations

Lorem ipsum.

5. IANA Considerations

Lorem ipsum.

6. References

6.1. Normative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC8901] Huque, S., Aras, P., Dickinson, J., Vcelak, J., and D. Blacka, "Multi-Signer DNSSEC Models", RFC 8901, DOI 10.17487/RFC8901, September 2020, <https://www.rfc-editor.org/info/rfc8901>.

6.2. Informative References

[KEYTRAP] Heftrig, E., Schulmann, H., Vogel, N., and M. Waidner, "The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNS", <https://www.athene-center.de/fileadmin/content/PDF/Keytrap_2401.pdf>.

Authors' Addresses

Mark Andrews
Internet Systems Consortium
Email: marka@isc.org

Shumon Huque
Salesforce
Email: shuque@gmail.com

Yorgos Thessalonikefs
NLnet Labs
Email: yorgos@nlnetlabs.nl