Network Working Group
Internet-Draft
Updates: 9432 (if approved)
Intended status: Standards Track
Expires: 27 October 2025

K. Dyson
Nominet UK

25 April 2025

Initialisation of DNSSEC Policy for DNS Catalog Zones Members
draft-dyson-dnssec-policy-initialisation-00

Abstract

This document describes an update to "DNS Catalog Zones" ([RFC9432]) that facilitates a method to signal DNSSEC policy to DNSSEC signers for member zone(s) using information contained within a catalog zone.

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/.

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 27 October 2025.

Table of Contents

1. Introduction

This document is a companion to draft-dyson-primary-zonefile-initialisation in that between them, and in conjunction with "DNS Catalog Zones" ([RFC9432]) and "Dynamic Updates in the Domain Name System (DNS UPDATE)" ([RFC2136]), it becomes possible to complete the end to end initialisation of the provisioning, distribution, signing and serving of a new zone using standards-defined mechanisms.

The key steps covered are:

* Dynamically add a new zone to a catalog ("DNS Dynamic Updates" ([RFC2136]), "DNS Catalog Zones" ([RFC9432]))

* Have a designated primary server initialise the zone and serve it (draft-dyson-primary-zonefile-initialisation)

* Have secondary servers automatically add and transfer the zone ("DNS Catalog Zones" ([RFC9432]))

* Have designated DNSSEC signer(s) initialise keys and signing policy for the zone (this document)

Operators of large scale DNS systems may want to be able to signal the creation of keys as well as key lifetime and other DNSSEC related policy parameters as part of an end-to-end automated mechanism. Further, they may want to avoid the need or overhead of engineering a bespoke solution with the ongoing need to support and maintain it.

This document defines a vendor-independent mechanism of signalling DNSSEC policy parameters to DNSSEC signer(s) consuming a catalog zone.

Broader provisioning of the base nameserver configuration is beyond the scope of this document.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following is in addition to the conventions and definitions as defined in "DNS Catalog Zones" ([RFC9432]).

The use of parenthesis in the examples is as described in "Domain Names - Implementation and Specification" ([RFC1035]) Section 5.1.

3. Catalog Zone Properties

This section specifies new Catalog Zone level properties, additional to those defined in "DNS Catalog Zones" ([RFC9432]).

3.1. Schema Version (version property)

For this memo, the value of the version.$CATZ TXT resource record is unchanged.

"DNS Catalog Zones" ([RFC9432]) Section 3 is clear that "Catalog consumers MUST ignore any RRs in the catalog zone for which no processing is specified or which are otherwise not supported by the implementation." and as such the addition of the records outlined in this document will be ignored by implementations that do not recognise them.

3.2. DNSSEC (dnssec property)

If the catalog zone consumer is configured to be a signer of the member zone being processed, the server MUST apply the policy in the catalog. This action does not have to be constrained to the point at which a member zone is newly added to the catalog zone. If a catalog zone is re-configured such that signing is added or updated, the policy MUST be applied to existing members zones within the catalog.

If the server consuming the catalog zone is not configured to be a signer for the member zones in the catalog, records within the bailiwick of the dnssec property record MUST be ignored.

The "dnssec" property and labels within that bailiwick are OPTIONAL and if absent then no special processing relating to DNSSEC should occur.

A number of sub-properties, expressed as labels within the bailiwick of the "dnssec" label, define the initialisation parameters.

3.2.1. Enabling Signing (enabled property)

The "enabled" property is used to signal whether zones should be signed.

It is OPTIONAL and if absent, defaults to "1".

This can be configured at both the catalog zone level, as well as at the member zone level. As such, it facilitates the ability to set policy parameters at the catalog level, and then override that setting on a per member zone level.

3.2.1.1. Parameters

The only parameter is a boolean, stored as a character-string in the RDATA of a TXT resource record.

3.2.1.2. Examples

Signing is disabled by default for member zones:

```
enabled.dnssec.$CATZ IN TXT "0"
```

Signing is enabled by default for member zones:

```
enabled.dnssec.$CATZ IN TXT "1"
```

3.2.2. Policy (policy property)

If the implementation has the concept of pre-configured DNSSEC policy, the "policy" property can be used to indicate the name of such a policy.

The "policy" property is OPTIONAL. If present, then its value takes priority over policy defined in the catalog.

If the named policy is not configured on the designated signing server, then an error SHOULD be logged. DNSSEC related processing MAY continue if the other dnssec properties are present and correct. Otherwise, processing SHOULD continue as if the entire dnssec property section was absent.

Note that the member zone section permits the catalog zone level settings to be overridden. A global policy can be overridden with either a different policy, or with key details at the member zone level (see Section 4).

3.2.2.1. Parameters

The only parameter is a character-string in the RDATA of a TXT resource record containing name of the pre-configured policy.

3.2.2.2. Example

```
policy.dnssec.$CATZ IN TXT "some-dnssec-policy-name"
```

3.2.3. Keys (key property)

The "key" property is used to configure keys that will be applied to the member zone(s) in the catalog.

In the case of a single combined key (type csk), at least one key MUST be defined.

In the case of split keys (types zsk, ksk), at least one key of each type MUST be defined.

If parameters are omitted, such as key sizes or timing parameters, sensible defaults following the guidance of "DNSSEC Operational Practices, Version 2" ([RFC6781]) MUST be used.

3.2.3.1. type parameter

The "type" parameter MUST be present, and is used to convey the key type. It MUST be one of csk, zsk or ksk

3.2.3.2. alg parameter

The "alg" parameter MUST be present, and is used to convey the key algorithm. Algorithms can be specified by name or number (see IANA Registry "DNS Security Algorithm Numbers").

3.2.3.3. bits parameter

The "bits" parameter is OPTIONAL, depending on whether this is relevant to the algorithm being used.

3.2.3.4. lifetime parameter

The "lifetime" parameter is OPTIONAL and is used to specify how long the key should be published for before being rolled.

A value of zero (0) is used to indicate "unlimited" whereby the key will not be rolled. This is also the default if unspecified.

3.2.3.5. Examples

Combined Key

```
key.dnskey.$CATZ IN TXT "type=csk alg=RSASHA256 bits=2048 lifetime=0"
```

Split Key. The KSK will have unlimited lifetime due to the omitted lifetime parameter defaulting to zero (0). The ZSK will have a lifetime of 90 days.

```
key.dnssec.$CATZ IN TXT "type=ksk alg=ECDSAP256SHA256"
key.dnssec.$CATZ IN TXT "type=zsk alg=ECDSAP256SHA256 lifetime=90D"
```

3.2.4. Non Existence (nsec property)

The nsec parameter is OPTIONAL.

If absent, it defaults to the value "nsec".

3.2.4.1. Parameters

The only parameter is a character-string in the RDATA of a TXT resource record containing the preferred NSEC mechanism.

If the desired mechanism is NSEC3, the NSEC3 parameters MAY be supplied immediately after, separated by a space. If supplied, they MUST be compliant with "DNSSEC Security (DNSSEC) Hashed Authenticated Denial of Existence" ([RFC5155]) Section 3.3.

If the value is set to "nsec3" and the NSEC3 parameters are omitted, the values MUST default to "1 0 0 -" as per "Guidance for NSEC3 Parameter Setting" ([BCP236]) Section 3.1.

3.2.4.2. Examples

NSEC

```
nsec.dnssec.$CATZ IN TXT "nsec"
```

NSEC3 with defaults from [BCP236]

```
nsec.dnssec.$CATZ IN TXT "nsec3"
```

NSEC3 with supplied parameters

```
nsec.dnssec.$CATZ IN TXT "nsec3 1 1 0 aabbccdd"
```

4. Member Zone Properties

The default properties outlined above can be overridden per member zone. If properties are specified in a more specific scope than the defaults, the most specific scope MUST be used.

A subset MAY be specified in a more specific scope, for example, the SOA could be omitted, and just the NS records or DNSSEC parameters specified.

The omitted properties would be inherited from the catalog level values.

Similarly, if parameters for a property are defined at the catalog zone level, and only some parameters are overridden at the member zone level, the other parameters SHOULD be inherited from the catalog zone level.

```
<unique-N>.zones.$CATZ          0 PTR example.com.
enabled.dnssec.<unique-N>.zones.$CATZ IN TXT "1"
key.dnssec.<unique-N>.zones.$CATZ IN TXT ( "type=csk"
        "alg=ECDSAP256SHA256" )
nsec.dnssec.<unique-N>.zones.$CATZ IN TXT "nsec3"
```

4.1. Change Of Ownership (coo property)

There is no change to the coo property; if the member zone changes ownership to another catalog, fundamentally, the zone’s master file already exists.

The scope of this document is solely concerned with the initialisation of a new zone's master file, and so in the case of the zone changing ownership, the initialisation parameters MUST NOT be processed.

Noting that the primary server for a given catalog's member zones may not be the primary server for the catalog zone itself, nor the primary server for another catalog's member zones, operators should consider their implementation's configuration when planning a change of ownership operation.

5. Name Server Behaviour

5.1. General Behaviour

5.2. Member Zone Removal

If the member zone is removed from the catalog zone, then any data or configuration related to the DNSSEC signing of the zone MUST also be removed unless the implementation provides a configuration option that facilitates retention.

5.3. Zone-Associated State Reset

In the event of a zone state reset being carried out, the state of the zone's master file MUST be reset as if the file was being initialised for the first time per this document.

6. Implementation and Operational Notes

When configuring the use of catalog zones, implementations should give the operator the ability to indicate whether the catalog zone consumer is a DNSSEC signer of the catalog's member zones.

7. Security Considerations

This document does not alter the security considerations outlined in "DNS Catalog Zones" ([RFC9432]).

8. IANA Considerations

IANA is requested to add the following entries to the registry:

Registry Name: DNS Catalog Zones Properties

Reference: this document

Property Prefix	Description	Status	Reference
dnssec	DNSSEC Properties	Standards Track	this document
enabled.dnssec	Enable/Disable DNSSEC Signing	Standards Track	this document
policy.dnssec	DNSSEC Policy	Standards Track	this document
key.dnssec	DNSSEC Keys	Standards Track	this document
nsec.dnssec	DNSSEC Proof of Non Existence	Standards Track	this document

Table 1: DNS Catalog Zones Properies Registry

Field meanings are unchanged from the definitions in "DNS Catalog Zones" ([RFC9432]).

9. Normative References

[BCP236] Best Current Practice 236, <https://www.rfc-editor.org/info/bcp236>. At the time of writing, this BCP comprises the following:

Hardaker, W. and V. Dukhovni, "Guidance for NSEC3 Parameter Settings", BCP 236, RFC 9276, DOI 10.17487/RFC9276, August 2022, <https://www.rfc-editor.org/info/rfc9276>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/rfc/rfc2136>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/rfc/rfc5155>.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <https://www.rfc-editor.org/rfc/rfc6781>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9432] van Dijk, P., Peltan, L., Sur簞, O., Toorop, W., Monshouwer, C.R., Thomassen, P., and A. Sargsyan, "DNS Catalog Zones", RFC 9432, DOI 10.17487/RFC9432, July 2023, <https://www.rfc-editor.org/rfc/rfc9432>.

Appendix A. Examples

A.1. Catalog Zone Example

The following is an example catalog zone showing some of the additional properties and parameters as outlined in this document.

By default, zones are signed with ECDSAP256SHA256, and NSEC is used for proof of non existence.

The example.com zone is not signed at all.

The example.org zone is signed with RSASHA256 with 2048 bit keys.

The example.net zone is signed with NSEC3 with OptOut set.

```
catz.invalid.                    0 SOA invalid. invalid. (
      1 3600 600 2419200 3600 )
catz.invalid.                    0 NS invalid.
enabled.dnssec.catz.invalid.     0 TXT "1"
key.dnssec.catz.invalid.         0 TXT ( "type=zsk"
      "alg=ECDSAP256SHA256" )
key.dnssec.catz.invalid.         0 TXT ( "type=ksk"
      "alg=ECDSAP256SHA256" )
nsec.dnssec.catz.invalid.        0 TXT "nsec"
kahdkh6f.zones.catz.invalid.     0 PTR example.com.
hajhsjha.zones.catz.invalid.     0 PTR example.net.
ytrytryt.zones.catz.invalid.     0 PTR example.org.
enabled.dnssec.kahdkh6f.zones.catz.invalid. 0 TXT "0"
key.dnssec.ytrytryt.zones.catz.invalid. 0 TXT ( "type=zsk"
     "alg=RSASHA256 bits=2048" )
key.dnssec.ytrytryt.zones.catz.invalid. 0 TXT ( "type=ksk"
     "alg=RSASHA256 bits=2048" )
nsec.hajhsjha.zones.catz.invalid. 0 TXT "nsec3 1 1 0 -"
```

Appendix B. Author Notes/Thoughts

NB: To be removed by the RFC Editor prior to publication.

More parameters can be added to support timings, TTLs, etc, but I wanted to circulate the broad idea for feedback first before refining the detail.

Not sure referring to BCP236 by section is correct as if the BCP is updated to refer to another RFC, the section reference may be incorrect... suspect I should remove the section reference...

I’ve stated that at least one key of each type MUST be configured, 1xCSK or (1xZSK + 1xKSK) however, this doesn’t permit for the scenario where the operator keeps their KSK offline and only periodically signs and re-inserts the keyset signature into the zone...

It may also be nice to be able to say "type=none" so that if the zone received is already signed, it can be unsigned... see other operator/ transition thought below...

I’m mindful of this being useful, but also not overly complex. It’s outside of the scope of this document, for example, as to the updating of the DS in the parent. There are other mechanisms, such as RFC9615 that deal with this.

I'm also mindful that 3.2 says that if the policy changes, it must be applied to member zones - this feels like it is open to causing mayhem unless the operator is very careful. I'd like to include something like the word "gracefully" ('the policy MUST be gracefully applied') but this feels too wooly and unclear. I'd welome thoughts here.

I've stated that if defined, the name of a pre-defined (in the implementation's config, such as BIND9's dnssec-policy) policy name should override policy defined in the catalog, but then permitted keys to be defined at a member zone level. This may be confusing. I'm thinking about revising/removing this.

I'm thinking about defining named policy in the catalog and then setting a default named policy at the catalog level and just specifying the policy name at the mmeber zone level if there's a desire to override.

so, something like:

```
key.dnssec.mypolicy.policies.dnssec.catz.invalid. 0 TXT ( "type=csk"
            "alg=13" )
nsec.dnssec.mypolicy.policies.dnssec.catz.invalid. 0 TXT "nsec3"
key.dnssec.otherpolicy.policies.dnssec.catz.invalid. 0 TXT ( "type=csk"
            "alg=8 bits 2048" )
nsec.dnssec.otherpolicy.policies.dnssec.catz.invalid. 0 TXT "nsec3 1 1 0 -"

enabled.dnssec.catz.invalid. 0 TXT "1"

policy.dnssec.catz.invalid. 0 TXT "mypolicy"
policy.dnssec.<unique-N>.zones.catz.invalid. 0 TXT "otherpolicy"
```

An operator may want to be able to transition zones from other operators without breaking DNSSEC; secondary the given zone from the existing provider, unsign it whilst post-publishing the incumbent's key(s) and re-sign with their own key(s) (all as part of a wider process). This feels quite niche and custom though, but is a use case I'm considering.

Appendix C. Change Log

NB: To be removed by the RFC Editor prior to publication.

C.1. 00 - Initial draft

Acknowledgments

TODO acknowledge.

Author's Address

Karl Dyson
Nominet UK
Minerva House
Edmund Halley Road
Oxford Science Park
Oxford
OX4 4DQ
United Kingdom
Email: karl.dyson@nominet.uk
URI: https://nominet.uk