DNSOP Working Group
Internet-Draft
Updates: 9432 (if approved)
Intended status: Standards Track
Expires: 28 September 2026

A. Suhonen
TREX
W. Toorop
NLnet Labs
A. Buddhdev
RIPE NCC
K. Dyson
Nominet UK
A. Sargsyan
Internet Systems Consortium

27 March 2026

DNS Catalog Zone Properties for Zone Transfers
draft-axu-dnsop-catalog-zone-xfr-properties-02

Abstract

This document specifies DNS Catalog Zones Properties that define the primary name servers from which specific or all member zones can transfer their associated zone, as well as properties related to zone transfers such as access control.

This document also defines a groups property, for the apex of the catalog zone, as a location to assign the additional properties to certain catalog zone groups.

Besides the additional properties, this document updates RFC9432 by explicitly allowing CNAME and DNAME records.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-axu-dnsop-catalog-zone-xfr-properties/.

Discussion of this document takes place on the dnsop Working Group mailing list (mailto:dnsop@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnsop/. Subscribe at https://www.ietf.org/mailman/listinfo/dnsop/.

Source for this draft and an issue tracker can be found at https://github.com/DNS-Hackathon/catalog-extensions-draft.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

DNS Catalog Zones [RFC9432] described a method for automatic DNS zone provisioning among DNS name servers by the catalog of zones to be provisioned as one or more regular DNS zones. Configuration associated with the member zones, such as from which primary name servers and with which TSIG keys [RFC8945] to transfer the zones, and from which IP addresses and with which TSIG keys DNS notifies [RFC1996] are allowed, were assumed to be preprovisioned at the catalog consumer.

This document specifies DNS Catalog Zones Properties to specify primary name servers from which to transfer the member zones, as well as properties to specify which IP addresses, using which cryptographic keys, are allowed to notify the secondary name server serving the member zones, in order to:

* remove the necessity to preprovision those at the catalog consumers,

* to facilitate ad-hoc changes, and

* to facilitate exceptions for individual member zones.

1.1. Requirements language

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.

2. Catalog Zone Structure

The new properties, specified in Section 4, MAY be at the apex of the catalog zone, where they will affect all member zones, or under a member zone label, where they will affect just that member zone. Any property under a member zone label will override that same property at the apex, which, in its turn, MAY override any default value coming from the configuration file. If the catalog consumer's configuration does not allow overriding its default values by a catalog zone (e.g., because of security considerations), then the catalog consumer SHOULD communicate to the operator (e.g., through a log message) information about the properties that are ignored because of the configuration.

When a property is overriden, the new property replaces all RRs of the old property. For example, both TXT and AAAA RRs defined at the apex are ignored for ZONELABEL1, but not ignored for ZONELABEL2, because ZONELABEL2 does not override the primaries property:

```
label.primaries.$CATZ            0 IN AAAA 2001:db8:35::53
label.primaries.$CATZ            0 IN TXT "TSIG key"

ZONELABEL1.zones.$CATZ           0 IN PTR example.com.
primaries.ZONELABEL1.zones.$CATZ 0 IN A 192.0.2.53

ZONELABEL2.zones.$CATZ           0 IN PTR example.net.
```

2.1. Binding additional attributes

It is possible to distinguish groups of values with all the properties from Section 4, by adding an additional label before the property. This allows binding additional attributes within the group, for example binding TSIG keys to certain IP addresses.

2.2. CNAME and DNAME Records

This document updates [RFC9432] by explicitly allowing CNAME [RFC1035] and DNAME [RFC6672] anywhere in the catalog. The CNAME and DNAME RRs in a catalog zone MUST refer to names within the same (catalog) zone. When a CNAME and DNAME RRs refer to owner names outside of the (catalog) zone, they MUST be considered invalid and MUST be ignored.

For example, using some of the properties from Section 4:

```
ZONELABEL1.zones.$CATZ                0 IN PTR example.com.
ZONELABEL1.zones.$CATZ                0 IN DNAME (
                                           customer1.config.$CATZ )

primaries.customer1.config.$CATZ      0 IN A 192.0.2.53
primaries.customer1.config.$CATZ      0 IN TXT "TSIG key"
allow-transfer.customer1.config.$CATZ 0 IN CNAME (
                                          internal.acls.config.$CATZ )

internal.acls.config.$CATZ            0 IN APL ( 1:10.0.0.0/8
                                           2:fd00:0:0:0:0:0:0:0/8 )
```

3. Schema Version (version property)

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

Section 3 of DNS Catalog Zones [RFC9432] 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.

4. New Properties

4.1. Primaries

This property defines which server(s) the member zone(s) will be fetched from. The RR types on this property MUST be either A or AAAA. If there are multiple RRs, the order in which they are used or tried is undefined. The order may be used following the default selection process in use by the catalog consumer name server software.

Different primaries MAY be distinguished by an additional label, which will allow binding additional attributes to each server.

```
primaries.$CATZ                   0 IN A 192.0.2.53

ZONELABEL1.zones.$CATZ            0 IN PTR example.com.
primaries.ZONELABEL1.zones.$CATZ 0 IN AAAA 2001:db8:35::53
```

If there are any RRs attached to the primaries that are not defined by this document, they SHOULD be ignored.

4.1.1. TSIG Key Name

The primaries property, with or without the extra label, MAY also have a TXT resource record set (RRset), which MUST consist of a single TXT RR, which will contain the name of the TSIG key to use to protect zone transfers. The key(s) MUST be defined elsewhere, such as in the configuration file of the consumer. If the key cannot be found, the consumer MUST NOT attempt a zone transfer from the name server addresses for which the TXT RRset was an additional attribute. A TXT RRset for a primaries property containing more than a single TXT RR indicates a broken catalog zone that MUST NOT be processed (see Section 5.1 of [RFC9432]).

```
ZONELABEL2.zones.$CATZ                0 IN PTR example.net.
ns1.primaries.ZONELABEL2.zones.$CATZ 0 IN AAAA 2001:db8:35::53
ns1.primaries.ZONELABEL2.zones.$CATZ 0 IN TXT "keyname-for-ns1"
ns2.primaries.ZONELABEL2.zones.$CATZ 0 IN AAAA 2001:db8:35::54
ns2.primaries.ZONELABEL2.zones.$CATZ 0 IN TXT "keyname-for-ns2"
```

4.1.2. Signalling encrypted transports

The primaries property, _with_ the extra label, MAY also have a TLSA RRset with one or more TLSA RRs [RFC6698]. The presence of a TLSA RRset signals support of DNS over TLS (DoT) [RFC7858] or DNS over QUIC (DoQ) [RFC9250] by the primary and the means by which the catalog consumer can successfully authenticate the primary. TLSA RRsets MUST be prepended by two labels (below the property label _with_ the extra label) indicating the decimal representation of the port number (see Section 3 of [RFC6698]) and the protocol name of the transport (see Section 4 of [I-D.draft-ietf-dnsop-svcb-dane-05]). Catalog consumers MUST transfer member zone and incremental updates over either DoT or DoQ in the presence of a TLSA RRset.

An authentication domain name (see Section 2 of [RFC8310]) MAY be provided by a PTR RRset, which MUST consist of a single PTR RR, at the same name as the TLSA RRset. When an authentication domain name is provided, catalog consumer MUST send the TLS SNI extension containing that name.

For the same reasons as given in Section 3.1.3 of [RFC7672], the TLSA RRs with certificate usage PKIX-TA(0) or PKIX-EE(1) SHOULD NOT be included. Catalog consumers SHOULD treat such RRs as "unusable" and ignore the affected primaries property. Catalog consumers SHOULD also communicate the error to the operator (e.g., through a log message).

```
ZONELABEL2.zones.$CATZ                              0 IN PTR example.net.
ns1.primaries.ZONELABEL2.zones.$CATZ                0 IN AAAA (
                                                        2001:db8:35::53 )
_853._quic.ns1.primaries.ZONELABEL2.zones.$CATZ     0 IN PTR (
                                                       ns1.example.net. )
_853._quic.ns1.primaries.ZONELABEL2.zones.$CATZ     0 IN TLSA (
                                                  3 1 1 \<SHA-256 pin\> )
```

4.2. Notify

This property MAY be used to define the DNS NOTIFY [RFC1996] message sending behavior of the consumer for the target zone(s). A and AAAA RRsets list hosts that the consumer will send DNS NOTIFY messages to when it loads a new version of the target zone(s).

An additional label below the property name MAY be used to distinguish different groups of addresses, which will allow binding additional attributes to each group.

4.2.1. TSIG Key Name

The notify property, with or without the extra label, MAY also have a TXT RRset, which MUST consist of a single TXT RR, which will contain the name of the TSIG key to use to sign the NOTIFY message. The key(s) MUST be defined elsewhere, such as in the configuration file of the consumer. If the key cannot be found, the consumer MUST NOT notify the name server addresses for which the key was an additional attribute. A TXT RRset for a notify property containing more than a single TXT RR indicates a broken catalog zone that MUST NOT be processed (see Section 5.1 of [RFC9432]).

```
notify.$CATZ                        0 IN A 192.0.2.49
notify.$CATZ                        0 IN TXT "name-of-default-key"

ZONELABEL3.zones.$CATZ              0 IN PTR example.org.
notify.ZONELABEL3.zones.$CATZ       0 IN AAAA 2001:db8:35::53
notify.ZONELABEL3.zones.$CATZ       0 IN TXT "keyname-for-ns4"

ns5.notify.ZONELABEL4.zones.$CATZ 0 IN AAAA 2001:db8:35::54
ns5.notify.ZONELABEL4.zones.$CATZ 0 IN TXT "keyname-for-ns5"
```

If there are any RRs attached to the notify property that are not defined by this document, they SHOULD be ignored.

4.3. Allow Query

The allow-query property MAY be used to define an access list of hosts or networks that are allowed to send queries for the target zone(s). The property MAY contain a RRset of type APL [RFC3123], which MUST consist of only a single APL RR. The prefixes listed in the APL RR are processed in order: - An IP address is allowed to query the zone when it matches a prefix. - An IP address is denied to query the zone when it matches a negated prefix.

The absence of an allow-query property at both apex of the catalog as well as at a member zone, means that the default policy applies, which may be that the member zone is allowed to be queried from any IP address without TSIG key.

Additional attributes (such as TSIG keys) can be bound to specific APL RRs by an additional label below the property label. The prefixes (with or without attributes) will be processed in Section 6 of canonical order [RFC4034], which means that the RRsets at the allow-query property label will be processed first, followed by the RRsets with the additional label in canonical order. When a catalog consumer encounters an APL RRset containing more that a single APL RR, it MUST be interpreted as an APL RRset containing a single APL RR denying all IP addresses, i.e.: APL !1:0.0.0.0/0 !2:0:0:0:0:0:0:0/0.

4.3.1. TSIG Key Name

The allow-query property MAY also have a TXT RRset, which will (further) restrict the zone to be queryable only with the TSIG keys indicated in any of the TXT RRs in the set. The key(s) MUST be defined elsewhere, such as in the configuration file of the consumer.

If a TXT RRset is present together with an APL RR, then first the policies in the APL are applied, and if that results in queries being allowed for the IP address, then in addition a TSIG key MUST match any of the TXT RRs in the TXT RRset. If a TXT RRset is present without an APL RRset, then only a TSIG key MUST match in any of the TXT RRs in the TXT RRset, regardless of the querying IP address.

If an allow-query property is present _and_ contains APL RRsets and/or TXT RRsets (either directly below the property label or below the additional label), _and_ none of the ACLs and/or TSIG keys matched or could be found, then the consumer MUST NOT allow queries for the member zone to which the property applies.

```
ZONELABEL5.zones.$CATZ                              0 IN PTR (
                                                          example.local. )
00-internal.allow-query.ZONELABEL5.zones.$CATZ 0 IN APL (
                                  1:10.0.0.0/8 2:fd00:0:0:0:0:0:0:0/8 )
50-external.allow-query.ZONELABEL5.zones.$CATZ 0 IN TXT "keyname"
```

4.4. Allow Transfer

The allow-transfer property MAY be used to define an access list of hosts or networks that are allowed to transfer the target zone(s) from the consumer. The property MAY contain a RRset of type APL [RFC3123], which MUST consist of only a single APL RR. The prefixes listed in the APL are processed in order: - An IP address is allowed to query the zone when it matches a prefix. - An IP address is denied to query the zone when it matches a negated prefix.

The absence of an allow-transfer property at both apex of the catalog as well as at a member zone, signifies that transfers of the zone from the consumer MUST NOT be allowed. Additional attributes (such as TSIG keys) can be bound to specific APL RRs by an additional label below the property label. The prefixes (with or without attributes) will be processed in Section 6 of canonical order [RFC4034], which means that the RRsets at the allow-transfer property label will be processed first, followed by the RRsets with the additional label in canonical order. When a catalog consumer encounters an APL RRset containing more that a single APL RR, it MUST be interpreted as an APL RRset containing a single APL RR denying all IP addresses, i.e.: APL !1:0.0.0.0/0 !2:0:0:0:0:0:0:0:0/0.

4.4.1. TSIG Key Name

The allow-transfer property MAY also have a TXT RRset, which will (further) restrict the zone to be transferable only with the TSIG key indicated in any of the TXT RRs in the set. The key(s) MUST be defined elsewhere, such as in the configuration file of the consumer. If a TXT RRset is present together with an APL RR, then first the policies in the APL are applied, and if that results in transfers being allowed for the IP address, then in addition a TSIG key MUST match any of the TXT RRs in the TXT RRset. If a TXT RRset is present without an APL RRset, then only a TSIG key MUST match in any of the TXT RRs in the TXT RRset, regardless of the querying IP address.

If an allow-transfer property is present _and_ contains APL RRsets and/or TXT RRsets (either directly below the property label or below the additional label), _and_ none of the APLs and/or TSIG keys matched or could be found, then the consumer MUST NOT allow transfers of the member zone to which the property applies.

```
ZONELABEL5.zones.$CATZ                                0 IN PTR (
                                                        example.local. )
00-internal.allow-transfer.ZONELABEL5.zones.$CATZ 0 IN APL (
                                  1:10.0.0.0/8 2:fd00:0:0:0:0:0:0:0/8 )
50-external.allow-transfer.ZONELABEL5.zones.$CATZ 0 IN TXT "keyname"
```

If there are RRs other than APL, CNAME, or TXT attached to the allow-transfer property, or if neither an APL RR, nor a TXT RR can be found and there is also no CNAME that points to a meaningful RR (APL or TXT), then the most restrictive access list possible SHOULD be assumed.

5. Assigning properties to groups

It is possible to assign the properties from this document to catalog groups (see Section 4.3.2. of [RFC9432]). To this end this document introduces the groups property.

5.1. Groups (the groups property)

The list of catalog groups that have properties assigned to it, is specified as a collection of member nodes represented by TXT RRs under the owner name "groups" where "groups" is a direct child domain of the catalog zone. The names of member zones are represented on the RDATA side of a TXT record (instead of being represented as a part of owner names) so that all valid group names may be represented. This TXT record MUST be the only record in the TXT RRset with the same name. The presence of more than one record in the RRset indicates a broken catalog zone that MUST NOT be processed (see Section 5.1. of [RFC9432]). For example, if a catalog zone lists two catalog groups ("foo" and "bar"), the member node RRs would appear as follows:

```
<unique-1>.groups.$CATZ 0 IN TXT "foo"
<unique-2>.groups.$CATZ 0 IN TXT "bar"
```

where <unique-N> is a label that tags each record in the collection and has a unique value. When different <unique-N> labels hold the same TXT value (i.e., provide more than a single place to assign properties to the same group), the catalog zone is broken and MUST NOT be processed (see Section 5.1. of [RFC9432]).

Properties assigned to a catalog group, below an entry below the groups property extends the configuration that was already associated with that group. If the existing configuration for the group had a configuration value that is also targeted with property assigned for the group, then the assigned property's value MUST override the original value. If there was no existing group yet, then an entry below the groups property defines the new group.

6. Implementation and Operational Notes

One of the rationales for allowing CNAME and DNAME records is that a large and complex catalog may have large and complex access lists repeated many times. But if there are only a few different access lists, they could be defined separately and then be referenced many times, reducing both the size and processing effort of the catalog zone.

Alternatively, a group property may be used for this, which will or will not have additional properties assigned to it under the groups property (see Section 5).

7. IANA Considerations

IANA is requested to add the following entries to the "DNS Catalog Zones Properties" registry under the "Domain Name System (DNS) Parameters" page:

Property Prefix	Description	Status	Reference
groups	List of catalog groups	Standards track	[this document]
primaries	Primary name servers	Standards Track	[this document]
notify	Send DNS NOTIFY behavior	Standards track	[this document]
allow-transfer	Allow zone transfer from	Standards track	[this document]
allow-query	Allow queries from	Standards track	[this document]

Table 1

8. Implementation Status

[NOTE to the RFC Editor: Please remove this section before publication]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft [RFC7942].

The existing BIND 9 implementation of primaries, allow-transfer and allow-query was a major inspiration for writing this draft.

9. Security and Privacy Considerations

The original RFC for Catalog Zones already covers a lot of security and privacy considerations, and they are all still valid, but there are also new security considerations introduced by this document.

9.1. Private Zone Exfiltration

If the Catalog Zone producer and consumer are different organizations, the producer may be able to use a crafted Catalog Zone to exfiltrate a private zone on another server within the consumer's network by listing it in the Catalog Zone with more permissive query or transfer access lists. The producer needs to know the exact name of the private zone and an address of the primary where the consumer may fetch it from.

There are two ways to approach this security issue. One is to make sure that the consumer organisation does not allow zone transfers for private zones on the consuming server. Another approach is to sanitize the incoming Catalog Zone before consuming it, removing anything sensitive from it.

10. References

10.1. Normative References

[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>.

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <https://www.rfc-editor.org/rfc/rfc1996>.

[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>.

[RFC3123] Koch, P., "A DNS RR Type for Lists of Address Prefixes (APL RR)", RFC 3123, DOI 10.17487/RFC3123, June 2001, <https://www.rfc-editor.org/rfc/rfc3123>.

[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/rfc/rfc4034>.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, DOI 10.17487/RFC6672, June 2012, <https://www.rfc-editor.org/rfc/rfc6672>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/rfc/rfc6698>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <https://www.rfc-editor.org/rfc/rfc7672>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/rfc/rfc7858>.

[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>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/rfc/rfc8310>.

[RFC8945] Dupont, F., Morris, S., Vixie, P., Eastlake 3rd, D., Gudmundsson, O., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", STD 93, RFC 8945, DOI 10.17487/RFC8945, November 2020, <https://www.rfc-editor.org/rfc/rfc8945>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

[RFC9432] van Dijk, P., Peltan, L., Sur篁, 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>.

10.2. Informative References

[I-D.draft-ietf-dnsop-svcb-dane-05] Schwartz, B. M. and R. Evans, "Using DNSSEC Authentication of Named Entities (DANE) with DNS Service Bindings (SVCB) and QUIC", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-dane-05, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-dane-05>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/rfc/rfc7942>.

Appendix A. Example Catalog with One of Everything

```
   primaries.$CATZ                          0 IN A 192.0.2.53

   ZONELABEL1.zones.$CATZ                   0 IN PTR example.com.
   primaries.ZONELABEL1.zones.$CATZ         0 IN AAAA 2001:db8:35::53

   ZONELABEL2.zones.$CATZ                   0 IN PTR example.net.
   ns1.primaries.ZONELABEL2.zones.$CATZ     0 IN AAAA 2001:db8:35::53
   ns1.primaries.ZONELABEL2.zones.$CATZ     0 IN TXT "keyname-for-ns1"
   ns2.primaries.ZONELABEL2.zones.$CATZ     0 IN AAAA 2001:db8:35::54
   ns2.primaries.ZONELABEL2.zones.$CATZ     0 IN TXT "keyname-for-ns2"

   notify.$CATZ                             0 IN A 192.0.2.49

   ZONELABEL3.zones.$CATZ                   0 IN PTR example.org.
   notify.ZONELABEL3.zones.$CATZ            0 IN AAAA 2001:db8:35::53
   notify.ZONELABEL3.zones.$CATZ            0 IN TXT "no default notifies"

   ZONELABEL4.zones.$CATZ                   0 IN PTR sub.example.org.
   notify.ZONELABEL4.zones.$CATZ            0 IN AAAA 2001:db8:35::54
   notify.ZONELABEL4.zones.$CATZ            0 IN TXT ""

   ZONELABEL5.zones.$CATZ                   0 IN PTR example.local.
   allow-query.ZONELABEL5.zones.$CATZ       0 IN APL 1:10.0.0.0/8 (
                                    !1:0.0.0.0/0 !2:0:0:0:0:0:0:0/0 )
   allow-transfer.ZONELABEL5.zones.$CATZ 0 IN APL !1:0.0.0.0/0 (
                                                  !2:0:0:0:0:0:0:0/0 )
```

Acknowledgements

Thanks everybody who helped making this work possible.

Contributors

Thanks to all of the contributors.

Authors' Addresses

Aleksi Suhonen
TREX Regional Exchanges Oy
Kuninkaankatu 30 A
FI-33200 Tampere
Finland
Email: i-d-2025@ssd.axu.tm

Willem Toorop
NLnet Labs
Science Park 400
1098 XH Amsterdam
Netherlands
Email: willem@nlnetlabs.nl

Anand Buddhdev
RIPE NCC
Stationsplein 11
1012 AB Amsterdam
Netherlands
Email: anandb@ripe.net

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

Aram Sargsyan
Internet Systems Consortium
Email: aram@isc.org