User Documentation on Delegating and Redelegating a Generic Top-Level Domain (gTLD)

Table of Contents

Delegating a generic top-level domain

This document provides a guide to the generic top-level domain (gTLD) delegation process.

What is a delegation request?

As part of the responsibilities for managing the root zone, ICANN's IANA department is responsible for receiving requests to delegate domains in the DNS root zone. Note that this process is distinct from the process used to apply to be eligible for a new gTLD.

The delegation process results in the "NS" records being placed in the DNS root zone to make the domain active in the domain name system. This then facilitates the registry operator to commence the process to bring the registry service into production.

Submitting a delegation request

At the conclusion of the evaluation process for a new gTLD, i.e. following contract execution and pre-delegation testing by ICANN, a the registry operator will be provided with a unique delegation token and URL to ICANN's IANA Root Zone Management (RZM) site for new gTLD delegations.

Registry operators that are ready to commence a request for delegation must visit the RZM site and enter their token in order to commence the procedure.

At the start of the procedure, the registry operator or its agent (requestor) is asked to provide an email address to serve as a contact point for the life of the request. This email address will be validated to ensure it works correctly.

Following this, the requestor will be asked to provide details on the sponsoring organisation (i.e. contracted party), its designated administrative and technical contacts, and its technical configuration. The requirements for these elements are the same as for other types of root zone changes. The request will follow the routine change processing steps as defined below. In addition to following the routine steps, a delegation report will be sent to the ICANN Board and the Root Zone Administrator.

Tracking status

Once a request has been lodged, an applicant can revisit the delegation page with their token in order to be provided with a view of the current status of their requests. Any questions regarding the process can be directed to root-mgmt@iana.org.

Review of Delegation Steps

Step 1	After Pre-Delegation testing has been successfully completed, the requester receives unique, secure credentials to initiate a request within the automated Root Zone Management (RZM) System.
Step 2	Requester uses provided credentials and URL to login to the RZM System.

Step 3	Requester provides a contact email address for use with the request. In order to confirm the email address works, a link will be emailed to it, and the requestor should follow the link to proceed.
Step 4	Requester completes form in RZMS including the fields for the following: Manager: Also known as the "Registry" or "Sponsoring Organization", this is the organization to which responsibility for the domain is delegated. Administrative and Technical Contacts: These are contact points for the domain, responsible for responding to pubic enquiries concerning the domain, and also for authorising routine updates to the domain. Name servers/DS Records: This is the list of authoritative name servers maintained by the registry to serve the top-level domain, along with the delegation signer records for DNSSEC. Registration Information: Additional information pertaining to the domain, such as the location of its WHOIS server, and a web address where registration can be found.
Step 5	The request will go through the steps described in the "Routine Root Zone Change Request" described below.

Redelegating a generic top-level domain

This is a guide to the generic top-level domain (gTLD) redelegation process. This process is used when the IANA Root Zone Database must be updated to reflect a change in the management of a gTLD. The primary requirement of this process is to have an existing contract with ICANN, which reflects the changes related to the management of the gTLD.

To update the Root Zone Database to reflect a change to the registry operator for a gTLD, the registry must first secure an executed amendment to its Registry Agreement in accordance with its contractual obligations with ICANN. Once completed, a root zone change request should be filed according to the routine change process defined below.

During processing of the change request, ICANN's IANA department will confirm with ICANN's new gTLD team that the request accurately reflects the currently contracted party for the given gTLD. (Note that this process differs from the redelegation process for a country-code top-level domain.) The request will follow the routine change processing steps as defined below. In addition to following the routine steps, a delegation report will be sent to the ICANN Board and the Root Zone Administrator.

Review of Redelegation Steps

Step 1	Complete necessary contract amendments reflecting the change with ICANN
Step 2	Requester submits a root zone change request changing the relevant fields for the TLD in the Root Zone Database with new information. These include: Manager: Also known as the "Registry" or "Sponsoring Organization", this is the organization to which responsibility for the domain is delegated. Administrative and Technical Contacts: These are contact points for the domain, responsible for responding to pubic inquiries concerning the domain, and also for authorising routine updates to the domain. Name servers/DS Records: This is the list of authoritative name servers maintained by the registry to serve the top-level domain, along with the delegation signer records for domains that are DNSSEC secured. Registration Information: Additional information pertaining to the domain, such as the location of its WHOIS server, and a web address where registration can be found, can also be listed for a top-level domain. The root zone change request can be initiated through the RZM System if the requester has credentials. If not, the Delegation Request Form (link to form in document) can be used.
Step 3	The request will go through the steps described in the "Routine Root Zone Change Request" described below. During processing, Root Zone Management staff will verify that the proposed changes match the current contractual language for the TLD.

Routine Root Zone Change Request Process

Methods for submitting a routine request

An online interface is provided at https://rzm.iana.org for TLD managers to submit change requests. ICANN recommends that all TLD managers use this method if possible, as it will guide you through the process, provide immediate online feedback of potential issues, and offer the fastest processing time.

Processing a routine request

Once a request is received, it will go through the following processing steps:

Pre-review	The request is reviewed to ensure it is complete and clear. If it is not clear, clarification is sought from the requestor.
Technical testing	Any changes that are technical in nature will be validated against the relevant technical requirements. Any deficiencies are reported back to the requestor to fix. See: Technical requirements for root zone changes
Contact confirmation	The contact persons for the domain will be asked to agree to the changes.
Manual review	ICANN staff will review the request to ensure it is in accordance with any special obligations and other known regulatory requirements.
Delegation evaluation	If the request is deemed to represent a substantial change of control of the TLD, it is considered a redelegation request, and must be assessed according to the criteria of that process.
Supplemental technical testing	The technical tests are performed a second time, to ensure no new technical issues have arisen during the time the request was being processed
Authorisation	The details of the request are transmitted to the U.S. Department of Commerce for authorisation.

Implementation	Once implementation of a change request is authorised, the changes are implemented in the Root Zone and the Root Zone Database.

During processing of the request, the requestor will receive email updates relating to the status of the request. At any time, the contacts for the domain can log in to our web interface to check the status of the request.

Delegation Request Form

This is to be used as part of submitting a delegation or redelegation of a country-code top-level domain.

IANA TLD MODIFICATION TEMPLATE 2010-02-17

** This should be completed and submitted to root-mgmt@iana.org.
** In most cases, this can be completed online. For more information
** visit http://www.iana.org/domains/root/ or contact IANA for
** assistance.

1. Top-Level Domain Name.....:

2. Purpose of change.....:

Manager
3a. Organisation Name.....:
3b. Street Address.....:
3c. City.....:
3d. State.....:
3e. Postal Code.....:
3f. Country Code (2 letter).....:

Administrative Contact
4a. Contact Person's Name.....:
4b. Job Title.....:
4c. Organisation Name.....:
4d. Street Address.....:
4e. City.....:
4f. State.....:
4g. Postal Code.....:
4h. Country Code (2 letter).....:
4i. Phone Number.....:
4j. Fax Number.....:
4k. Email Address.....:
4l. Treat as role acct? (y/n).....:

Technical Contact
5a. Contact Person's Name.....:
5b. Job Title.....:
5c. Organisation Name.....:
5d. Street Address.....:
5e. City.....:
5f. State.....:
5g. Postal Code.....:
5h. Country Code (2 letter).....:
5i. Phone Number.....:
5j. Fax Number.....:
5k. Email Address.....:
5l. Treat as role acct? (y/n).....:

Authoritative Name Server
6a. Hostname.....:
6b. IP Address(es).....:

Authoritative Name Server (duplicate for additional name servers)
6a. Hostname.....:
6b. IP Address(es).....:

Delegation Signer Record (for DNSSEC signed zones only)
7a. Key Digest.....:
7b. Key Tag.....:
7c. Key Algorithm.....:
7d. Key Digest Type.....:

Delegation Signer Record (duplicate for additional DS records)
7a. Key Digest.....:
7b. Key Tag.....:
7c. Key Algorithm.....:
7d. Key Digest Type.....:

Domain Information
8a. URL for Registration Services...:
8b. WHOIS Server.....:

Special notes (for staff processing change, does not appear publicly)

9. Notes.....:

Technical requirements for authoritative name servers

This article describes the baseline technical conformance criteria for authoritative name servers. These are evaluated by ICANN as the IANA functions operator for changes to delegations in the DNS root zone.

Definitions

1. For purposes of this document, an authoritative name server is a DNS server that has been designated to answer authoritatively for the designated zone, and is being requested to be listed in the delegation. It is recorded by its fully-qualified domain name, potentially along with its IP addresses.

2. Name server tests are completed against each unique tuple of a hostname, an IP address, and a protocol. If a hostname has multiple IP addresses, for example, the tests will be conducted against each IP address.

Detailed requirements

Minimum number of name servers

There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.

Valid hostnames

The hostnames used for the name servers must comply with the requirements for valid hostnames described in RFC 1123, section 2.1.

Name server reachability

The name servers must answer DNS queries over both the UDP and TCP protocols on port 53. Tests will be conducted from multiple network locations to verify the name server is responding.

Answer authoritatively

The name servers must answer authoritatively for the designated zone. Responses to queries to the name servers for the designated zone must have the “AA”-bit set.

This will be tested by querying for the SOA record of the designated zone with no “RD”-bit set.

Network diversity

The name servers must be in at least two topologically separate networks. A network is defined as an origin autonomous system in the BGP routing table. The requirement is assessed through inspection of views of the BGP routing table.

Consistency between glue and authoritative data

For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.

Consistency between delegation and zone

The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.

Consistency between authoritative name servers

The data served by the authoritative name servers for the designated zone must be consistent.

All authoritative name servers must serve the same NS record set for the designated domain.

All authoritative name servers must serve the same SOA record for the designated domain.

If for operational reasons the zone content fluctuates rapidly, the serial numbers need only be loosely coherent.

No truncation of referrals

Referrals from the parent zone's name servers must fit into a non-EDNS0 UDP DNS packet and therefore the DNS payload must not exceed 512 octets.

The required delegation information in the referral is a complete set of NS records, and the minimal set of requisite glue records. The response size is assessed as a response to a query with a maximum-sized QNAME.

The minimal set of requisite glue records is considered to be:

> One A record, if all authoritative name servers are in-bailiwick of the parent zone; and,
>
> One AAAA record, if there are any IPv6-capable authoritative name servers and all IPv6-capable authoritative name servers are in-bailiwick of the parent zone.

Prohibited networks

The authoritative name server IP addresses must not be in specially designated networks that are either not globally routable, or are otherwise unsuited for authoritative name service.

0.0.0.0/8	Not globally routable	RFC 5735
10.0.0.0/8	Not globally routable	RFC 5735
100.64.0.0/10	Not globally routable	RFC 6598
127.0.0.0/8	Not globally routable	RFC 5735

169.254.0.0/16	Not globally routable	RFC 5735
172.16.0.0/12	Not globally routable	RFC 5735
192.0.2.0/24	Not globally routable	RFC 5735
192.88.99.0/24	6to4	RFC 3068
192.168.0.0/16	Not globally routable	RFC 5735
198.18.0.0/15	Not globally routable	RFC 5735
198.51.100.0/24	Not globally routable	RFC 5737
203.0.113.0/24	Not globally routable	RFC 5737
224.0.0.0/3	Not globally routable	RFC 5735
::/128	Not globally routable	RFC 5156
::1/128	Not globally routable	RFC 5156
::FFFF:0:0/96	IPv4 mapped addresses	RFC 4291
2001:2::/48	Not globally routable	RFC 5156

2001::/32	Teredo	RFC 4380
2001:10::/28	Not globally routable	RFC 5156
2001:DB8::/32	Not globally routable	RFC 5156
2002::/16	6to4	RFC 3056
FC00::/7	Not globally routable	RFC 5156
FE80::/10	Not globally routable	RFC 5156

No open recursive name service

The authoritative name servers must not provide recursive name service. This requirement is tested by sending a query outside the jurisdiction of the authority with the “RD”-bit set.

Same source address

Responses from the authoritative name servers must contain the same source IP address as the destination IP address of the initial query.

DS record format

Trust anchors must be provided each with the four attributes of a DS record — the key tag, the key algorithm, the digest hash type, and the digest hash. They must be provided with legal values for each of the DS record fields. For the hash digest, ICANN supports two types — SHA1 (value 1), and SHA256 (value 2).

Matching DNSKEY

At the time of the listing request, there must be a DNSKEY that matches the DS record present in the child zone. This will be tested for as part of the implementation of the record. As with most technical conformance criteria for the root zone, if a top-level domain operator has a situation where this is not the case, but this is by design and can be demonstrated not to affect the stability of the TLD or the root zone, it is possible to request that the DS records be listed regardless.

Validation of RRSIG

ICANN must be able to validate the RRSIG records returned for the zone based upon the DS record set that has been provided for the root zone. We test this by querying the apex SOA for the top-level domain with the DO bit set, and validating the SOA record against the proposed DS resource set.

Useful References

For more information on some of the key DNS technical concepts referenced by these technical tests, please look at the following references:

Domain Names — Concepts and Facilities (RFC 1034)

Domain Names — Implementation and Specification (RFC 1035)

Preventing Use of Recursive Nameservers in Reflector Attacks (RFC 5358)

Operational Considerations and Issues with IPv6 DNS (RFC 4472)

Extension Mechanisms for DNS (EDNS0) (RFC 2671)

DNS Referral Response Size Issues

DNS Transport over TCP - Implementation Requirements (RFC 5966)

IANA IPv6 Special Purpose Address Registry

Special-use IPv6 Addresses (RFC 5156)

Special-use IPv4 Addresses (RFC 5735)