The ALT Special Use Top Level Domain
draft-wkumari-dnsop-alt-tld-01

Abstract

This document reserves a string (ALT) to be used as a TLD label in non-DNS contexts. It also provides advice / guidance to developers developing alternate namespaces.

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 October 18, 2014.

Copyright Notice

Copyright (c) 2014 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.
1. Introduction

Many protocols and systems need to name entities. The DNS "standard" of a series of labels separated with dots has become common, even in systems that are not actually part of the DNS.

This document reserves the string "ALT" (short for Alternate) as a Special Use Domain ([RFC6761]) that should be used in the right-most label position to signify that this name is not rooted in the DNS, and that normal registration and lookup rules do not apply.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Terminology

This document assumes familiarity with DNS terms and concepts. Please see [RFC1034] for background and concepts.

- DNS context: The namespace administered by ICANN. This is the namespace / context that "normal" DNS uses.

- non-DNS context: Any other / alternate namespace.
2. Background

The DNS is a tree, and so has a single root. Conventionally, a name immediately beneath the root is called a "Top Level Domain" or "TLD". TLDs usually delegate portions of their namespace to others, who may then delegate further. The hierarchical, distributed and caching nature of the DNS has made it the primary resolution system on the Internet.

The success of the DNS makes it a natural starting point for systems that need to name entities in a non-DNS context. These name resolutions occur in a namespace distinct from the DNS. A number of good examples of these sorts of systems are documented in Special-Use Domain Names of Peer-to-Peer Systems [I-D.grothoff-iesg-special-use-p2p-names].

In many cases, these systems build a DNS style tree parallel to the global DNS administered by IANA. They often use a pseudo-TLD to cause resolution in this alternate namespace, using browser plugins, shims in the name resolution process, or simply applications that only use this alternate namespace.

In many cases the creators of these alternate namespaces have simply chosen a convenient / descriptive string and started using this. These new strings are "alternate" strings, and not actually registered anywhere or part of the DNS. However they appear to be TLDs, as they are the in the right-most position of a name. Issues may arise if they are looked up in the DNS. These include:

- **User confusion:** If someone emails a link of the form foo.bar.pseudo-TLD to someone who does not have the necessary software to resolve names in the pseudo-TLD namespace, they may become confused.

- **Excess traffic hitting the DNS root.** Lookups may leak out of the pseudo-TLD namespace and end up hitting the DNS root nameservers.

- **Collisions:** If the pseudo-TLD is eventually delegated from the root zone the behavior may be non-deterministic.

- **Lack of success for the user’s original goal.**

One of the primary design goals of a number of these alternate name resolution systems is to provide confidentiality of the names being resolved.

A significant number of these alternate name resolution systems are specifically designed to provide confidentiality of the looked up
name, and provide a distributed and censorship resistant namespace. For example, the Tor project use of .onion is intended to provide a confidential and alternate name resolution process. This goal may be defeated if the queries leak into the DNS, for example if a Tor user shares a link with a friend who doesn't have the Tor browser installed.

3. The ALT namespace

In order to avoid the above issues we reserve the .ALT label. This label should be used as a pseudo-TLD (in the right most (TLD) position of a name) to signify that this is an alternate (non-DNS) namespace.

Alternate namespaces should differentiate themselves from other alternate namespaces by choosing a name and using it in the label position just before the pseudo-TLD. For example, a group wishing create a namespace for Friends Of Olaf they may choose the string "foo" and use any set of labels under foo.alt.

As they are in an alternate namespace they have no significance in the regular DNS context and so should not be looked up in the DNS context. Unfortunately simply saying that "something should not happen" doesn't actually stop it from happening, so we need some rules to deal with these.

1. Stub resolvers MAY elect not to send queries to any upstream resolver for names in the ALT TLD.

2. Iterative resolvers SHOULD follow the advice in [RFC6303], Section 3.

3. The root zone nameservers should either return NXDOMAIN responses, or the ALT TLD should be delegated to "new style" AS112 nameservers.

Groups wishing to create alternate namespaces SHOULD create their alternate namespace "under" a label that names their namespace, and "under" the ALT label. They SHOULD choose a label that they expect to be unique / descriptive. As there is no registry for the ALT namespace uniqueness is not guaranteed.

Currently deployed projects and protocols that are using pseudo-TLDs (for example, the ".onion" pseudo-TLD (and other labels in [I-D.grothoff-iesg-special-use-p2p-names]) are not expected to move under the ALT TLD (but may do so if they wish; this is a common resource). Rather, the ALT TLD is being reserved so that future projects of a similar nature have a designated place to create
alternate resolution namespaces that will not conflict with the
regular DNS context.

A number of names other than .ALT were considered and discarded. In
order for this technique to be effective the names need to continue
to followed the DNS format (a prime consideration for alternate name
formats be that they can be entered in places that normally take DNS
context names), this rules out using suffixes that are not themselves
DNS labels. Another proposal was that the ALT TLD instead be a
reservation under .arpa. This was considered, but rejected because
of we are suggesting that this be served as an [RFC6303] and that
recursive operators configure themselves to serve empty authoritative
zones for the reserved labeled. There is a concern that if there
were placed under .arpa less experienced nameserver operators may
inadvertently cover .arpa. A more significant concern is that the
scope of the issue if the query does leak, and the fact that this
would then make the root of the alternate naming namespace a third
level domain, and not a second one. A project may be willing to have
a name of the form example.alt, but example.alt.arpa may be not look
as good [TODO: Better wording here. Don’t want to say "vanity" !]

4. Advice to developers

An option would be for name resolution systems that operate outside
to DNS to "root" themselves under a DNS name that the project or
organization controls. So, for example if the Tor project controls
tor.example.com it could "root" their namespace under
onion.tor.example.com. The concept of "rooting" a non-DNS context in
da DNS context requires some explanation. This document tries to
mitigate collisions in the DNS context. This means that if a name
from the alternate naming system gets resolved in the DNS, it should
not conflict or cause unexpected behavior. By "rooting a non-DNS
context namespace in the DNS context, under a name controlled by the
project" we mean that the rightmost set of labels should, if resolved
in the DNS context be in a domain controlled by the developers /
project. This means that, in the above example the software
implementing the alternate namespace (browser plugins, custom stub
resolvers, etc) would then match on names that end in the string
"onion.example.com" and provide the alternate name resolution
(instead of matching on the strings ending in ".onion").

In a number of cases the purpose of the alternate name resolution
system is to provide confidentiality. For these systems the above
advice is problematic. If the a query for one of these names (for
example dissident.onion.example.com (this is not a real .onion
address)) were to leak into the DNS the query would hit the recursive
resolver, and (assuming empty caches) would then hit the root, the
.com name servers, the example.com name servers and then the
onion.example.com nameservers. This means that the fact that a user
is resolving disident.onion.example.com would be visible to a large
number of people. Furthermore, the onion.example.com nameservers
become a good oracle to determine what names exist, and who is trying
to reach them.

For projects that are very latency sensitive, or which desire to
provide confidentiality we recommend rooting the alternate namespace
under the .ALT TLD.

5. IANA Considerations

The IANA is requested to add the ALT string to the "Special-Use
Domain Name" registry ([RFC6761], and reference this document. In
addition, the "Locally Served DNS Zones" ([RFC6303]) registry should
be updated to reference this document.

[ Ed: There are two options here. Option 1: We could ask the IANA to
run a "First Come First Served" registry for labels under the ALT
TLD. By registry I mean a "standard" IANA registry, not a registry
in the DNS sense of the word (IANA would publish on a webpage "Foo |
fred@example.com | Used for the foo project"). Option 2: This is a
fully uncoordinated space (in the same way that people have been
picking pseudo-TLDs up till now) -- pick something that, as far as
you know others are not using... There are pros and cons to both -- I
don’t want to overload the IANA, have people stage a land-grab for
names, or give the impression that this is a "real" TLD. Thoughts?
Currently we say there is no registry (Section 3), but that can be
changed.]

6. Security Considerations

One of the motivations for the creation of the alt pseudo-TLD is that
unmanaged labels in the managed root name space are subject to
unexpected takeover if the manager of the root name space decides to
delegate the unmanaged label.

The unmanaged and registry-free nature of labels beneath .ALT
provides the opportunity for an attacker to re-use the chosen label
and thereby possibly compromise applications dependent on the special
host name.

7. Acknowledgements

The authors understand that there is much politics surrounding the
delegation of a new TLD and thank the ICANN liaison (and any other
poor sod who gets sucked into this) in advance.
8. References

8.1. Normative References

[I-D.grothoff-iesg-special-use-p2p-names]
Grothoff, C., Wachs, M., hellekin, h., and J. Appelbaum,
"Special-Use Domain Names of Peer-to-Peer Systems", draft-grothoff-iesg-special-use-p2p-names-02 (work in progress),
March 2014.


[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate

6303, July 2011.

RFC 6761, February 2013.

8.2. Informative References

[I-D.ietf-sidr-iana-objects]
Manderson, T., Vegoda, L., and S. Kent, "RPKI Objects
issued by IANA", draft-ietf-sidr-iana-objects-03 (work in progress), May 2011.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication ]

From -00 to -01.

  o Fixed the abstract.

  o Recommended that folk root their non-DNS namespace under a DNS
    namespace that they control (Joe Abley)

Authors’ Addresses
Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US
Email: warren@kumari.net

Andrew Sullivan
Dyn
150 Dow Street
Manchester, NH 03101
US
Email: asullivan@dyn.com