Special-Use Domain Names of Peer-to-Peer Systems

Document Version:
Accepted manuscript including changes made at the peer-review stage

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

draft-grothoff-iesg-special-use-p2p-names-00.txt
Internet Engineering Task Force (IETF)   C. Grothoff
Internet-Draft   M. Wachs
                                                               TU Munich
                                                         H. Wolf, editor
                                                           GNU consensus
                                                            J. Appelbaum
                                                        Tor Project Inc.
                                                           Nov 13, 2013

Intended status: (IESG Approval)
Expires: May 17th, 2014

            Special-Use Domain Names of Peer-to-Peer Name Systems

Abstract

   Today, the Domain Name System (DNS) is a key service for the
   Internet. DNS is primarily used to map human-memorable names to IP
   addresses, which are used for routing but generally not meaningful
   for humans. However, the hierarchical nature of DNS makes it
   unsuitable for various Peer-to-Peer (P2P) Name Systems. As
   compatibility with applications using DNS names is desired, these
   overlay networks often define alternative pseudo Top-Level Domains
   (pTLDs) to integrate names from the P2P domain into the DNS
   hierarchy.

   This memo describes common Special-Use Domain Names [RFC6761]
   pseudo Top-Level DNS Names designed to help harden name resolution
   security (e.g., [RFC6840][RFC6975]), provide censorship resistance,
   and protect the users' privacy on the Internet.

   In this IESG Approval document we are asking for domain name
   reservations for five Special-Use Domain Names [RFC6761] TLDs:
   ".gnu", ".zkey", ".onion", ".exit", and ".i2p".

Status of this Memo

   This is an IESG Approval document specification [RFC5226] defining
   special handling of the said five Special-Use Domain Names for
   Peer-to-Peer Name Systems, in conformance with the registration
   procedure defined in RFC 6761, section 4.

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."

1. Introduction

   [RFC6761] defines a mechanism for reserving DNS names for special
   use.

   This document is an IESG Approval document requesting the
   reservation of five pTLDs for special use: ".gnu", ".zkey",
   ".onion", ".exit", and ".i2p". They relate to peer-to-peer systems
   that, given their decentralized design, do not require a central
   authority to register names.

   The GNU Name System (GNS) (".gnu", ".zkey"), the Tor network
   (".onion", ".exit"), and the Invisible Internet Project (".i2p")
   use these pseudo-Top-Level Domains (pTLDs) to realize
   fully-decentralized and censorship-resistant secure alternatives
   for DNS or, in the case of the ".exit" pTLD, to control overlay
   routing and to securely specify path selection choices [TOR-PATH].

   To facilitate integration with legacy applications, the overlay's
   namespaces can be accessed from applications to resolve these
   special TLDs, for example via specialized SOCKS proxies [RFC1928],
   specialized DNS servers, or transparent name resolution and
   ephemeral address mapping.

   This document describes the proposed special treatment for each of
   these five pTLDs below following the questions from [RFC6761],
   section 5.

2. Terminology and Conventions Used in This Document

   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 "Key words for
   use in RFCs to Indicate Requirement Levels" [RFC2119].

   The word "peer" is used in the meaning of a individual system on
   the network. Thus, "local peer" means the localhost.

   The acronym "pTLD" is used as a shortcut to mean a pseudo Top-Level
   Domain, i.e., a name or label for a network not present in
   operational DNS, and not registered with IANA for use within the
   scope of operational DNS. Specifically, it refers to one of the
   Special-Use Domain Names already in use on the Internet and
   described in this document.

   In this document, ".tld" (with quotes) means: any domain or
   hostname within the scope of a given pTLD, while .tld (without
   quotes), or dot-tld, both refer to an adjective form. For example,
   a collection of ".gnu" peers, but an .onion URL. The pTLD itself

is mentioned with dot, and within double quotes, and usually
followed by the word pTLD.

The Tor-related names such as 'circuit', 'exit', 'node', 'relay',
'stream', and related Tor terms are described in [Dingledine2004]
and the Tor protocol specification [TOR-PROTOCOL].

3. Description of Special-Use Domains in P2P Networks

3.1. The ".gnu" Relative pTLD

The ".gnu" pTLD is used to specify that a domain name should be
resolved using GNS instead of DNS. The GNS resolution process is
documented in [Schanzenbach2012]. As GNS users need to install a
GNS resolver on their individual system and as GNS resolution does
not depend on DNS, there are no considerations for DNS with respect
to the internals of the GNS resolution process itself. Note that
".gnu" names SHOULD follow the naming conventions of DNS.

".gnu" names are personal, relative, and transitive: each user of
the GNS controls their own zone that is authoritative for all
".gnu" domains; zones can be delegated between authorities, so that
any user can share names, and chain labels to resolve names out of
the requesting user's zone of control, including across several
zones.

For example, if Alice wants to access the Web service of Bob's
friend Dave, she might be able to lookup: "www.dave.bob.gnu",
whereas Bob will simply ask for "www.dave.gnu" to obtain the same
result.

3.2. The ".zkey" Compressed Public Key pTLD

The ".zkey" pTLD is used to signify that resolution of the given
name MUST be performed using a record signed by an authority that
is in possession of a particular public key. Names in ".zkey" MUST
end with a domain which is the compressed point representation from
[EdDSA] on [Curve25519] of the public key of the authority, encoded
using base32hex [RFC4648]. A GNS resolver uses the key to locate a
record signed by the respective authority.

The ".zkey" pTLD provides a (reverse) mapping from globally unique
hashes to public key, therefore names in ".zkey" are non-memorable,
and are expected to be hidden from the user [Schanzenbach2012].

3.3. Geographically Anonymous pTLDs

The Tor anonymization network makes use of several special pTLD
domains, three of which have seen widespread usage to date
[TOR-ADDRESS].

3.3.1. The ".onion" Hidden Service pTLD

The widely deployed ".onion" pTLD designates an anonymous Tor Hidden
Service reachable via the Tor network [Dingledine2004]. These
.onion URLs are self-authenticating addresses for use with any TCP
service. Such addresses are typically resolved, reached and
authenticated through transparent proxying or through a local SOCKS
proxy running on TCP port 9050, TCP port 9150 or another user
selected TCP port. The purpose of the Tor Hidden Services system
is to provide geographic anonymity for the .onion host and for all

clients visiting the hidden service as well as other purposes such
as NAT traversal, strong authentication, anonymity and censorship
resistance.

Addresses in ".onion" are opaque, non-mnemonic, alpha-semi-numeric
hashes corresponding to an 80-bit truncated SHA1 hash over a given
Tor hidden service's public key. This hash can be made up of any
letter of the alphabet and decimal digits beginning with 2 and
ending with 7, thus representing a number in base32 [RFC4648]. Tor
generates this "Onion key" automatically when the hidden service is
configured. Tor clients use it following the Tor Rendezvous
specifications [TOR-RENDEZVOUS].

3.3.2. The ".exit" Client Source Routing pTLD

   The dot-exit suffix is used as an in-band source routing control
   channel, usually for selection of a specific Tor relay during path
   creation as the last node in the Tor circuit.

   It may be used to access a DNS host via specific Torservers, in the
   form "hostname.nickname-or-fingerprint.exit", where the "hostname"
   is a valid hostname, and the "nickname-or-fingerprint" is either
   the nickname of a Tor relay in the Tor network consensus, or the
   hex-encoded SHA1 digest of the given node's public key
   (fingerprint).

   For example, "gnu.org.noisetor.exit" will route the client to
   "gnu.org" via the Tor node nicknamed "noisetor". Using the
   fingerprint instead of the nickname ensures that the path selection
   uses a specific Tor exit node, and is harder to remember: e.g.,
   "gnu.org.f97f3b153fed6604230cd497a3d1e9815b007637.exit".

   When Tor sees an address in this format, it uses the specified
   "nickname-or-fingerprint" as the exit node. If no "hostname"
   component is given, Tor defaults to the published IPv4 address of
   the Tor exit node [TOR-EXTSOCKS].

3.3.3. The ".noconnect" Client Interruption pTLD

   The dot-noconnect suffix is used in Tor for testing purposes: when
   Tor sees an address in this format, it immediately closes the
   connection without attaching it to any circuits. It is useful for
   controllers that want to test whether a given application is indeed
   using the same instance of Tor that they're controlling.

   This is a deprecated pTLD and thus we do not include the
   ".noconnect" pTLD in the list of Special-Use Domain Names that
   should be reserved.

3.4. The ".i2p" Addressbook pTLD

   The ".i2p" pTLD provides accessibility to anonymous services
   ("eepsites") within the I2P network. I2P is a scalable,
   self-organizing, resilient packet switched anonymous network layer,
   upon which any number of different anonymity or security-conscious
   applications can operate.

   The local I2P proxy resolves such names either by looking up a
   local table called the addressbook, or by decoding Base32-encoded
   [RFC4648] public keys and establishing a tunnel to the respective
   authority, similar to contacting .onion hidden services.

I2P uses 52 characters (256 bits) of the SHA-256 hash of the public
key to identify eepsites [I2P-NAMING]. These identifiers can be
used to address a peer as, e.g.:
"ukeu3k5oycgaauneqgtnvselmt4yemvoilkln7jpvamvfx7dnkdq.b32.i2p".

Apart from the ".b32.i2p" domain that is reserved for SHA-256
hashes, other hostnames within the ".i2p." pTLD are
non-hierarchical and can be assigned locally: example.i2p and
other.example.i2p do not necessarily belong to the same authority.

As the system is decentralized, example.i2p may also resolve
differently for different peers, depending on the state of their
respective addressbooks.

4. Security Considerations

Specific software performs the resolution of the five requested
Special-Use Domain Names presented in this document; this
resolution process happens outside of the scope of DNS. Leakage of
requests to such domains to the global operational DNS can cause
interception of traffic that might be misused to monitor, censor,
or abuse the user's trust, and lead to privacy issues with
potentially dramatic consequences for the user.

Operation of said TLDs into the global DNS scope could as well
produce conflicts due to later real use and the possible
acquisition of intellectual property rights in such names.

The reservation of several Top-Level Domain names for these
purposes will minimize such confusion and conflict, and safety
risks for users.

5. IANA Considerations

The P2P Name Systems domains listed below, and any domains falling
within those domains are Special-Use Domain Names [RFC6761]:

      gnu.
      zkey.
      onion.
      exit.
      i2p.

5.1. Domain Name Reservation Considerations

The five domains listed above, and any names falling within those
domains (e.g., "example.gnu.", "j6im4v42ur6dpic3.onion.", etc.) are
special [RFC6761] in the following ways:

   1. Users MAY use these names as they would other DNS names,
   entering them anywhere that they would otherwise enter a
   conventional DNS name, or a dotted decimal IPv4 address, or a
   literal IPv6 address.

   Since there is no central authority responsible for assigning
   dot-gnu and dot-i2p names, and that specific domain is local to
   the local peer, users SHOULD be aware of that specificity.

   Since there is no central authority responsible for assigning
   dot-b32-dot-i2p, dot-onion, and dot-zkey names, and those names

match cryptographic keys, users SHOULD be aware that they don't
belong to regular DNS, but are still global in their scope.

In any case, resolution of the five proposed pTLDs is similar to
the normal DNS resolution, and thus SHOULD not affect normal
usage of most Internet applications.

2. Application Software MAY pass requests to any of the five
proposed pTLDs for normal DNS resolution if A/AAAA records are
desired. If available, the local DNS resolver MUST intercept
such requests within the respective operating system hooks and
behave like DNS. However, P2P-aware application MAY choose to
talk directly to the respective P2P resolver, and in the case of
GNS use this to access additional GNS-specific record types.

As mentioned in sections 4.1.4 and 4.1.5 below, regular DNS
resolution is expected to respond with NXDOMAIN for the five
proposed pTLDs. Therefore, if it can differentiate between DNS
and P2P name resolution, application software MAY expect such a
response, and MAY choose to treat other responses from the DNS
as errors.

3. Name Resolution APIs and Libraries MAY choose to support
additional GNS record types over time and MAY choose to directly
resolve those domains via a GNS-specific resolution protocol or
API. However, for legacy applications and legacy name
resolution APIs, no changes are required.

The ".onion" and ".i2p" pTLDs are typically accessed via HTTP or
SOCKS proxies and do not define additional record types.

4. If any request to one of the five considered pTLDs is sent to
the global operational DNS, the only valid answer from DNS is
NXDOMAIN. Therefore, a caching DNS server MUST respond with
NXDOMAIN. The caching DNS server MAY choose to cache that
response.

5. Authoritative DNS Servers are not expected to treat these
TLDs specially. In practice, they SHOULD answer with NXDOMAIN,
as none of the considered pTLDs are normally available via
global DNS resolution, and not doing so MAY put users' privacy
at risk, e.g., as suggested in the next point.

6. DNS Server Operators SHOULD treat requests to the five
considered pTLDs as typos, for correct installations MUST not
allow P2P requests to escape to DNS. DNS operators SHOULD NOT
choose to redirect such bogus requests to a site, not even to
explain to the user that their P2P resolver is missing or
mis-configured as this MAY violate privacy expectations of the
user.

7. DNS Registries/Registrars

In order to avoid conflicts with the P2P namespaces, IANA should
reserve all five considered pTLDs and forbid registrars from
registering domains names within their respective scopes.

6. Acknowledgements

The authors thank the I2P developers for their constructive
feedback, and Leif Ryge for his proof-reading and valuable

feedback.

7. References

7.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to
                      Indicate Requirement Levels", BCP 14, RFC 2119,
                      March 1997.

   [RFC5226]   Narten, T., Alvestrand, H., "Guidelines for
                      Writing an IANA Considerations Section in RFCs",
                      BCP 26, RFC 5226, May 2008.

   [RFC6761]   Cheshire, S. and M. Krochmal, "Special-Use Domain
                      Names", RFC 6761, February 2013.

7.2. Informative References

   Tor specifications are mentioned below with the TOR- prefix, and
   available from the Tor Project documentation page:
   https://www.torproject.org/docs/documentation.html#DesignDoc

   [Curve25519]   Bernstein, D.J., "Curve25519: new Diffie-Hellman
                      speed record", February 2006,
                      URL: http://cr.yp.to/ecdh/curve25519-20060209.pdf

   [Dingledine2004]   Dingledine, R., Mathewson, N., and Syverson, P.,
                      "Tor: the second-generation onion router", in
                      SSYM'04 Proceedings of the 13th conference on
                      USENIX Security Symposium - Volume 13, page 21,
                      2004.

   [EdDSA]   Bernstein, D.J., Duif, N., Lange, T., Schwabe, P.,
                      and Yang B-Y., "High-speed, high-security
                      signatures", September 2011.
                      URL: http://ed25519.cr.yp.to/ed25519-20110926.pdf

   [I2P-NAMING]   jrandom, "Naming in I2P and Addressbook",
                      URL: http://www.i2p2.de/naming.html

   [RFC1928]   Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas,
                      D., and L. Jones, "SOCKS Protocol Version 5", RFC
                      1928, March 1996.

   [RFC4648]   Josefsson, S., "The Base16, Base32, and Base64
                      Data Encodings", RFC 4648, October 2006.

   [RFC6840]   Weiler, S., Ed., and D. Blacka, Ed.,
                      "Clarifications and Implementation Notes for DNS
                      Security (DNSSEC)", RFC 6840, February 2013.

   [RFC6975]   Crocker, S. and S. Rose, "Signaling Cryptographic
                      Algorithm Understanding in DNS Security
                      Extensions (DNSSEC)", RFC 6975, July 2013.

   [Schanzenbach2012] Schanzenbach, M., "Design and Implementation of
                      a Censorship Resistant and Fully Decentralized
                      Name System", September 2012.
                      See also URL: https://gnunet.org/gns

   [TOR-ADDRESS]   Mathewson, N., Dingledine, R., "Special
                      Hostnames in Tor", September 2011.
                      [TO BE REMOVED:
 https://gitweb.torproject.org/torspec.git/blob/HEAD:/address-spec.txt]

   [TOR-EXTSOCKS]   Mathewson, N., Dingledine, R., "Tor's extensions
                      to the SOCKS protocol", September 2011.
                      [TO BE REMOVED:
 https://gitweb.torproject.org/torspec.git/blob/HEAD:/socks-extensions.txt]

   [TOR-PATH]   Mathewson, N., Dingledine, R., "Tor Path
                      Specification", April 2013.
                      [TO BE REMOVED:
 https://gitweb.torproject.org/torspec.git/blob/HEAD:/path-spec.txt]

   [TOR-PROTOCOL]   Dingledine, R., Mathewson, N., "Tor Protocol
                      Specification", November 2013.
                      [TO BE REMOVED:
 https://gitweb.torproject.org/torspec.git/blob/HEAD:/tor-spec.txt]

   [TOR-RENDEZVOUS]   Mathewson, N., Dingledine, R., "Tor Rendezvous
                      Specification", September 2013.
                      [TO BE REMOVED:
 https://gitweb.torproject.org/torspec.git/blob/HEAD:/rend-spec.txt]

8. Authors' Addresses

   Christian Grothoff
   Free Secure Network Systems Group
   Lehrstuhl fuer Netzarchitekturen und Netzdienste
   Boltzmannstrasse 3
   Technische Universitaet Muenchen
   D-85748 Garching bei Muenchen, Bayern

   Email: christian@grothoff.org

   Matthias Wachs
   Free Secure Network Systems Group
   Lehrstuhl fuer Netzarchitekturen und Netzdienste
   Boltzmannstrasse 3
   Technische Universitaet Muenchen
   D-85748 Garching bei Muenchen, Bayern

   Email: wachs@net.in.tum.de

   Hellekin O. Wolf

   Email: hellekin@gnu.org

   Jacob Appelbaum

   Email: jacob@appelbaum.net

This document expires on May 17th, 2014.
Comments are solicited and should be addressed to the authors.