Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 4, 2014

C. Grothoff
M. Wachs
TU Munich
H. Wolf, Ed.
GNU consensus
J. Appelbaum
Tor Project Inc.
March 03, 2014

Special-Use Domain Names of Peer-to-Peer Systems
draft-grothoff-iesg-special-use-p2p-names-02

Abstract

This is an IESG Approval document requesting the reservation of six Top-Level Domains for special use, in conformance with the registration procedure defined in RFC 6761, section 4.

Peer-to-Peer systems use specific decentralized mechanisms to allocate, register, manage, and resolve names. Those mechanisms operate entirely outside of DNS, independently from the DNS root and delegation tree. In order to avoid interoperability issues with DNS as well as to address security and privacy concerns, this document describes six pseudo Top-Level Domain names (pTLDs), reserved for special use.

The following six domains relate to security-focused peer-to-peer systems. They are: ".gnu", ".zkey", ".onion", ".exit", ".i2p", and ".bit".

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology and Conventions Used in This Document 3
3. Description of Special-Use Domains in P2P Networks 4
3.1. The ".gnu" Relative pTLD 4
3.2. The ".zkey" Compressed Public Key pTLD 4
3.3. Geographically Anonymous pTLDs 4
3.3.1. The ".onion" Hidden Service pTLD 4
3.3.2. The ".exit" Client Source Routing pTLD 5
3.4. The ".i2p" Addressbook pTLD 5
3.5. The ".bit" Timeline System pTLD 6
4. Security Considerations 6
5. IANA Considerations 7
5.1. Domain Name Reservation Considerations for ".gnu." 7
5.2. Domain Name Reservation Considerations for ".zkey." 8
5.3. Domain Name Reservation Considerations for ".onion." . . . 10
5.4. Domain Name Reservation Considerations for ".exit." 11
5.5. Domain Name Reservation Considerations for ".bit." 13
5.6. Domain Name Reservation Considerations for ".i2p." 14
6. Acknowledgements 15
7. References 15
7.1. Normative References 15
7.2. Informative References 15
Authors' Addresses 17

1. Introduction

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 domain names is desired, these overlay networks often define exclusive alternative pseudo Top-Level Domains (pTLDs) to avoid conflict between the P2P namespace and the DNS hierarchy.

The purpose of this document is to inform the Internet community about current practice of such pseudo-TLDs within peer-to-peer systems, and to normalize their usage according to the rules of RFC 6761. Given their decentralized design, such P2P systems do not require a central authority to register names nor do they belong to the DNS resolution tree.

RFC 6761 defines a mechanism for reserving domain names for special use. This document is an IESG Approval document requesting the reservation of six pTLDs for special use: ".gnu", ".zkey", ".onion", ".exit", ".i2p", and ".bit".

The GNU Name System (GNS) (".gnu", ".zkey"), the Tor network (".onion", ".exit"), the Invisible Internet Project (".i2p"), and the Dot-Bit Project (".bit") 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.

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 RFC 2119.

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 allocated using common DNS procedures, and reserved with IANA for special use.

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.

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 labels, 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].

Because "hostname" is allegedly valid, the total length of a dot-exit construct may exceed the maximum length allowed for domain names. Moreover, the resolution of "hostname" happens at the exit node. Trying to resolve such invalid domain names, including chaining dot-exit names will likely return a DNS lookup failure at the first exit node.

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. The details of I2P's operation [I2P-NAMING] are outside of the scope of this document.

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

3.5. The ".bit" Timeline System pTLD

The ".bit" pTLD provides a name space where names are registered via transactions in the Namecoin currency [Namecoin]. Like Bitcoins, Namecoins are created using a proof-of-work calculation, which is also used to establish a decentralized, multi-party consensus on the valid transaction history, and thus the set of registered names and their values [SquareZooko].

The Namecoin used in a transaction to register a name in ".bit" is lost. This is not a fundamental problem as more coins can be generated via mining (proof-of-work calculations). The registration cost is set to decrease over time, to prevent early adopters from registering too many names.

The owner of a name can update the associated value by issuing an update, which is a transaction that uses a special coin which is generated as change during the registration operation. If a name is not updated for a long time, the registration expires.

4. Security Considerations

Specific software performs the resolution of the six 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.

This RFC addresses another possible security concern, as the reservation of several Top-Level Domain names for these purposes will

minimize the possibility of confusion and conflict, and especially privacy 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.

bit.

5.1. Domain Name Reservation Considerations for ".gnu."

The ".gnu." domain is special according to RFC 6761, section 5 [RFC6761], in the following ways:

1. Users MAY use these names as they would other domain names, entering them anywhere that they would otherwise enter a conventional DNS domain name.

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

   In any case, resolution in the dot-gnu pTLD returns DNS compatible results, and thus SHOULD NOT affect normal usage of most Internet applications.

2. Application Software MAY pass requests for dot-gnu domains for normal DNS resolution. If available, the local resolver MUST intercept such requests within the respective operating system hooks and return DNS compatible results. However, GNS-aware applications MAY choose to talk directly to the respective GNS resolver, and use this to access additional record types (with numbers above 65535) that are not defined in DNS.

   As mentioned in points 4. and 5. below, regular DNS resolution is expected to respond with NXDOMAIN. 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. For legacy applications and legacy name resolution APIs expecting DNS resolution, no changes are required.

   However, Name Resolution APIs and Libraries MAY choose to support additional record types over time for the dot-gnu names. They MAY choose to directly resolve those domains via appropriate APIs or mechanisms such as the GNS-specific resolution protocol.

4. Caching DNS servers SHOULD recognize dot-gnu names as special and SHOULD NOT, by default, attempt to look up NS records for them, or otherwise query authoritative DNS servers in an attempt to resolve dot-gnu names. Instead, caching DNS servers SHOULD, by default, generate immediate negative responses for all such queries.

5. Authoritative DNS Servers are not expected to treat dot-gnu domain requests specially. In practice, they MUST answer with NXDOMAIN, as dot-gnu is not 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 dot-gnu domain as errors, for correct installations MUST NOT allow such requests to escape to DNS. DNS operators MUST NOT choose to redirect such 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 [SAC45], IANA reserves ".gnu." and thereby ensures that this label cannot be registered within the DNS tree, nor their management delegated to any particular organization.

5.2. Domain Name Reservation Considerations for ".zkey."

The ".zkey." domain is special according to RFC 6761, section 5 [RFC6761], in the following ways:

1. Users MAY use these names as they would other domain names, entering them anywhere that they would otherwise enter a conventional DNS domain name.

   Since there is no central authority necessary or possible for assigning dot-zkey names, and those names match cryptographic keys, users SHOULD be aware that they do not belong to regular DNS, but are still global in their scope.

   In any case, resolution in the dot-zkey pTLD returns DNS compatible results, and thus SHOULD NOT affect normal usage of most Internet applications.

2. Application Software MAY pass requests for dot-zkey domains for normal DNS resolution. If available, the local resolver MUST intercept such requests within the respective operating system hooks and return DNS compatible results. However, GNS-aware applications MAY choose to talk directly to the respective GNS resolver, and use this to access additional record types (with numbers above 65535) that are not defined in DNS.

   As mentioned in points 4. and 5. below, regular DNS resolution is expected to respond with NXDOMAIN. 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. For legacy applications and legacy name resolution APIs expecting DNS resolution, no changes are required.

   However, Name Resolution APIs and Libraries MAY choose to support additional record types over time for the dot-zkey names. They MAY choose to directly resolve those domains via appropriate APIs or mechanisms such as the GNS-specific resolution protocol.

4. Caching DNS servers SHOULD recognize dot-zkey names as special and SHOULD NOT, by default, attempt to look up NS records for them, or otherwise query authoritative DNS servers in an attempt to resolve dot-zkey names. Instead, caching DNS servers SHOULD, by default, generate immediate negative responses for all such queries.

5. Authoritative DNS Servers are not expected to treat dot-zkey domain requests specially. In practice, they MUST answer with NXDOMAIN, as dot-zkey is not 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 dot-zkey domain as errors, for correct installations MUST NOT allow such requests to escape to DNS. DNS operators MUST NOT choose to redirect such 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 [SAC45], IANA reserves ".zkey." and thereby ensures that this label cannot be registered within the DNS tree, nor their management delegated to any particular organization.

5.3. Domain Name Reservation Considerations for ".onion."

The ".onion." domain is special according to RFC 6761, section 5 [RFC6761], in the following ways:

1. Users MAY use these names as they would other domain names, entering them anywhere that they would otherwise enter a conventional DNS domain name.

   Since there is no central authority necessary or possible for assigning dot-onion names, and those names correspond to cryptographic keys, users SHOULD be aware that they do not belong to regular DNS, but are still global in their scope.

2. Application Software SHOULD NOT pass requests for dot-onion domains for normal DNS resolution.

   As mentioned in points 4. and 5. below, regular DNS resolution is expected to respond with NXDOMAIN. 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. For legacy applications, the only way to resolve dot-onion domains properly is via a SOCKS proxy. Using tools like TorSocks, SOCKS support can be added to legacy applications without changes to the application itself.

4. Caching DNS servers SHOULD recognize dot-onion names as special and SHOULD NOT, by default, attempt to look up NS records for them, or otherwise query authoritative DNS servers in an attempt to resolve dot-onion names. Instead, caching DNS servers SHOULD, by default, generate immediate negative responses for all such queries.

5. Authoritative DNS Servers are not expected to treat dot-onion domain requests specially. In practice, they MUST answer with NXDOMAIN, as dot-onion is not 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 dot-onion domain as errors, for correct installations MUST NOT allow such requests to escape to DNS. DNS operators MUST NOT choose to redirect such 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 [SAC45], IANA reserves ".onion." and thereby ensures that this label cannot be registered within the DNS tree, nor their management delegated to any particular organization.

5.4. Domain Name Reservation Considerations for ".exit."

The ".exit." domain is special according to RFC 6761, section 5 [RFC6761], in the following ways:

1. Users MAY use these names as they would other domain names, entering them anywhere that they would otherwise enter a conventional DNS domain name.

   Since dot-exit names correspond to a Tor-specific routing construct to reach target hosts via chosen Tor exit nodes, users

SHOULD be aware that they do not belong to regular DNS and that the actual target precedes the second-level domain name.

2. Application Software SHOULD NOT pass requests for dot-exit domains for normal DNS resolution.

   As mentioned in points 4. and 5. below, regular DNS resolution is expected to respond with NXDOMAIN. 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. For legacy applications, the only way to resolve dot-exit domains properly is via a SOCKS proxy. Using tools like TorSocks, SOCKS support can be added to legacy applications without changes to the application itself.

4. Caching DNS servers SHOULD recognize dot-exit names as special and SHOULD NOT, by default, attempt to look up NS records for them, or otherwise query authoritative DNS servers in an attempt to resolve dot-exit names. Instead, caching DNS servers SHOULD, by default, generate immediate negative responses for all such queries.

5. Authoritative DNS Servers are not expected to treat dot-exit domain requests specially. In practice, they MUST answer with NXDOMAIN, as dot-exit is not 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 dot-exit domain as errors, for correct installations MUST NOT allow such requests to escape to DNS. DNS operators MUST NOT choose to redirect such 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 [SAC45], IANA reserves ".exit." and thereby ensures that this label cannot be registered within the DNS tree, nor their management delegated to any particular organization.

5.5. Domain Name Reservation Considerations for ".bit."

The ".bit." domain is special according to RFC 6761, section 5 [RFC6761], in the following ways:

1. Users MAY use these names as they would other domain names, entering them anywhere that they would otherwise enter a conventional DNS domain name.

   From the user's perspective, the resolution of dot-bit pTLD 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 the dot-bit pTLD for normal DNS resolution if A/AAAA records are desired. If available, the local resolver MUST intercept such requests within the respective operating system hooks and return DNS compatible results. However, NameCoin-aware applications MAY choose to talk directly to the respective P2P resolver, and use this to access additional record types that are not defined in DNS.

3. For legacy applications and legacy name resolution APIs expecting DNS resolution, no changes are required.

   However, Name Resolution APIs and Libraries MAY choose to support additional record types over time for the dot-bit domain. They MAY choose to directly resolve those domains via blockchain-based resolution.

4. Caching DNS servers SHOULD recognize dot-bit names as special and SHOULD NOT, by default, attempt to look up NS records for them, or otherwise query authoritative DNS servers in an attempt to resolve dot-bit names. Instead, caching DNS servers SHOULD, by default, generate immediate negative responses for all such queries.

   Given that dot-bit users typically have no special privacy expectations, and those names are globally unique, local caching DNS servers MAY choose to treat them as regular domain names, and cache the responses obtained from the Namecoin blockchain. In that case however, NXDOMAIN results SHOULD NOT be cached, as new dot-bit domains may become active at any time.

5. Authoritative DNS Servers are not expected to treat dot-bit domain requests specially. In practice, they MUST answer with NXDOMAIN, as dot-bit is not available via global DNS resolution.

6. DNS Server Operators SHOULD treat requests to the dot-bit domain as errors, for correct installations SHOULD NOT allow such requests to escape to DNS.

7. DNS Registries/Registrars

   In order to avoid conflicts with the P2P namespaces [SAC45], IANA reserves ".bit." and thereby ensures that this label cannot be registered within the DNS tree, nor their management delegated to any particular organization.

5.6. Domain Name Reservation Considerations for ".i2p."

The ".i2p." domain is special according to RFC 6761, section 5 [RFC6761], in the following ways:

1. Users MAY use these names as they would other domain names, entering them anywhere that they would otherwise enter a conventional DNS domain name.

   Since there is no central authority responsible for assigning dot-i2p names, and that the ultimate mapping is decided by the local peer, users SHOULD be aware of that specificity.

2. Application Software SHOULD NOT pass requests for dot-i2p domains for normal DNS resolution.

   As mentioned in points 4. and 5. below, regular DNS resolution is expected to respond with NXDOMAIN. 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. For legacy applications, the only way to resolve dot-i2p domains properly is via a SOCKS proxy.

4. Caching DNS servers SHOULD recognize dot-i2p names as special and SHOULD NOT, by default, attempt to look up NS records for them, or otherwise query authoritative DNS servers in an attempt to

resolve dot-i2p names. Instead, caching DNS servers SHOULD, by default, generate immediate negative responses for all such queries.

5. Authoritative DNS Servers are not expected to treat dot-i2p domain requests specially. In practice, they MUST answer with NXDOMAIN, as dot-i2p is not 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 dot-i2p domain as errors, for correct installations MUST NOT allow such requests to escape to DNS. DNS operators MUST NOT choose to redirect such 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 [SAC45], IANA reserves ".i2p." and thereby ensures that this label cannot be registered within the DNS tree, nor their management delegated to any particular organization.

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. and H. Alvestrand, "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

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

[Dingledine2004]
Dingledine, R., Mathewson, N., and P. Syverson, "Tor: the second-generation onion router", 2004, <https://www.onion-router.net/Publications/tor-design.pdf>.

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

[I2P-NAMING]
Random, J., "Naming in I2P and Addressbook", 2003, <http://www.i2p2.de/naming.html>.

[Namecoin]
The .bit Project, "Namecoin DNS - DotBIT Project", 2013, <http://dot-bit.org/>.

[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.

[SAC45] ICANN Security and Stability Advisory Committee, "Invalid Top Level Domain Queries at the Root Level of the Domain Name System", November 2010, <http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf>.

[Schanzenbach2012]
Schanzenbach, M., "Design and Implementation of a Censorship Resistant and Fully Decentralized Name System", September 2012.

[SquareZooko]
Swartz, A., "Squaring the Triangle: Secure, Decentralized, Human-Readable Names", 2011, <http://www.aaronsw.com/weblog/squarezooko>.

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

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

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

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

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

Authors' Addresses

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

Email: christian@grothoff.org

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

Email: wachs@net.in.tum.de

Hellekin O. Wolf (editor)
GNU consensus

Email: hellekin@gnu.org

Jacob Appelbaum
Tor Project Inc.

Email: jacob@appelbaum.net