Independent Submission
Internet-Draft
Intended status: Best Current Practice
Expires: April 11, 2021

R. Arends
ICANN
J. Abley
Public Interest Registry

October 08, 2020

Top-level Domains for Private Internets
draft-dnsop-private-use-tld-00

Abstract

There are no defined private-use namespaces in the Domain Name System (DNS). For a domain name to be considered private-use, it needs to be future-proof in that its top-level domain will never be delegated from the root zone. The lack of a private-use namespace has led to locally configured namespaces with a top-level domain that is not future proof.

The DNS needs an equivalent of the facilities provided by BCP 5 (RFC 1918) for private internets, i.e. a range of short, semantic-free top-level domains that can be used in private internets without the risk of being globally delegated from the root zone.

The ISO 3166 standard is used for the definition of eligible designations for country-code top-level Domains. This standard is maintained by the ISO 3166 Maintenance Agency. The ISO 3166 standard includes a set of user-assigned code elements that can be used by those who need to add further names to their local applications.

Because of the rules set out by ISO in their standard, it is extremely unlikely that these user-assigned code elements would ever conflict with delegations in the root zone under current practices. This document explicitly reserves these code elements to be safely used as top-level domains for private DNS resolution.

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 https://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 April 11, 2021.

Table of Contents

1. Introduction 2
2. The ISO 3166-1 alpha-2 and Two-Letter Top-Level Domains . . . 4
3. ISO 3166-1 alpha-2 User-assigned Code Elements 4
4. Examples of Current Uses of the User-assigned Code Elements. 5
5. Private-use top-level Domains 8
6. IANA Considerations 9
7. Security Considerations 9
8. Acknowledgements 9
9. Informative References 9
Authors' Addresses 12

1. Introduction

In private networks where a hostname has no utility in the global namespace, it is convenient to have a private-use namespace. Such deployments could theoretically use sub-domains of a domain registered for the specific hosting entity, though not all such configurations have such a domain available. When the hostname is solely used in a private network, it is not necessary that it resolves globally.

Another situation is where applications use identifiers that are similar in appearance to domain names, and may be interpreted by software as domain names, but are not intended to use the global DNS resolution service. Using a private-use namespace helps guard against conflicts with the global DNS resolution system.

Note that a private-use namespace is not a subset of a registered special use namespace [IANA-Special]. There is no facility to register a specific label using the process defined in [RFC6761]. The process in RFC 6761 requires that a label has some kind of special handling in order to be considered special. A private-use namespace can be considered special on a policy level, but not on a technical or protocol level.

Many protocols outside the DNS have a defined set of elements for private use, or an identifier that indicates private use, such as "X-headers" MIME types [RFC2045], addresses for private internets [BCP-5], the "x-" sub-tag in private-use language tags [BCP-47], private-use Autonomous System Numbers [BCP-6], and private-use DNS RRTypes and RCODEs [BCP-42].

There is currently no such facility for the DNS namespace. A user is required to resort to registering a globally unique domain where a locally unique domain would suffice, or may configure a domain name that is not currently delegated from the root zone. Additionally, there are plenty of examples of device vendors that ship networking devices with a default setting for DHCP [RFC2131] option 15 (domain name) [RFC2132], containing a top-level domain that is believed to not be delegated in the root zone.

In practice, the lack of a private-use namespace facility has led to the deployment of arbitrary, unregistered, semantically meaningful top-level domains, such as ".home", ".dhcp", ".lan", ".localdomain", ".internal", ".dlink", ".ip" and ".corp" [ITHI]. These examples of locally configured strings are derived from traffic to the ICANN Managed Root Servers [IMRS] and are part of the most popular observed query names [BCP-219].

While these commonly chosen strings currently do not exist in the root zone, there is no guarantee that these strings will not be delegated in the root zone in the future. Therefore, there is no guarantee that the local use of these strings (or other strings that might be chosen for private use) will be stable, safe, and secure. Similarly, there is no guarantee that any of these strings will be deemed special-use via an application according to [RFC6761].

There are many uses for private-use names. It is not feasible to assign a semantically meaningful, relatively short top-level label to each individual private-use of a namespace in multiple languages. Similar to "X-headers" MIME types, and analogous in concept to address allocation for private internets, this document defines a range of abstract, two-letter labels that are aligned with the user-assigned two-letter code elements in the ISO 3166-1 alpha-2 [ISO3166-1] standard.

2. The ISO 3166-1 alpha-2 and Two-Letter Top-Level Domains

IANA's practice of governing the delegation of ASCII two-letter domain names in the DNS [STD13] root zone is to align it with assignment of two-letter (known as "alpha-2") code elements in the ISO 3166-1 standard [ISO3166-1]. The ISO 3166-1 standard contains many categories of code elements, with the "officially assigned" and some "exceptionally reserved" code elements being used in the DNS to represent entities as country-code top-level domains (ccTLDs) [RFC1591]. The interrelationship is documented in "ICANN and the ISO, A Common Interest in ISO Standard 3166" [ICANNISO].

In addition to the assigned, available, and reserved code elements, there are code elements designated as "user-assigned". The intent of user-assigned code elements is to provide the user with a code element when no other code element satisfies the intended use.

3. ISO 3166-1 alpha-2 User-assigned Code Elements

The ISO 3166-1 standard states in section 5.2:

> "In addition, exactly 42 alpha-2 code elements are not used in the ISO 3166, AA, QM to QZ, XA to XZ, ZZ."

And explains in clause 8.1 "Special Provisions":

> "Users sometimes need to extend or alter the use of country-code elements for special purposes. The following provisions give guidance for meeting such needs within the framework of this part of ISO 3166. "

And finally, clause 8.1.3 "User assigned code element":

> "If users need code elements to represent country names not included in this part of ISO 3166, the series of letters AA, QM to QZ, XA to XZ, and ZZ, and the series AAA to AAZ, QMA to QZZ, XAA to XZZ, and ZZA to ZZZ respectively and the series of numbers 900 to 999 are available. NOTE Users are advised that the above series of codes are not universals, those code elements are not compatible between different entities."

As shown above, the ISO 3166-1 user-assigned alpha-2 code elements are defined to be AA, QM to QZ, XA to XZ, and ZZ. The ranges ("to") are alphabetic and contain only characters in the US-ASCII definition [STD80].

It is unlikely that the user-assigned range will change.

4. Examples of Current Uses of the User-assigned Code Elements.

Using code elements to represent an entity other than a country name may appear to deviate from the intended use of the ISO 3166-1 standard. However, many organizations, including the IETF and the ISO, have used the user-assigned range to represent entities other than country names. The following list is not exhaustive but illustrates the wide variety of current uses of codes within the ISO 3166-1 user-assigned alpha-2 range.

- The International Standard Recording Code (ISRC) [ISO3901] uses code element "ZZ" from the User-assigned range for direct registrants independent of any country.

- The ISO Currency Codes standard [ISO4217] uses code elements "XA" to "XZ" from the user-assigned range for transactions and precious metals.

- International Securities Identification Numbers [ISO6166] uses the following code elements from the user-assigned range:

  QS: internally used by Euroclear France

  QT: internally used in Switzerland

  QW: internally used in WM Datenservice Germany for historical data

  XA: CUSIP Global Services substitute agencies

  XB: NSD Russia substitute agencies

  XC: WM Datenservice Germany substitute agencies

  XD: SIX Telekurs substitute agencies

  XF: internally assigned, non-unique numbers

  XS: Euroclear and Clearstream international securities

- The International Civil Aviation Organization [ICAO] Machine Readable Travel Documents standard uses code element "ZZ" from the user-assigned range for UN travel documents.

- The World Intellectual Property Organization [WIPO] Standard 3 uses the following code elements from the user-assigned range:

  QZ: Community Plant Variety Office (European Union) (CPVO).

XN: Nordic Patent Institute (NPI).

XU: International Union for the Protection of New Varieties of Plants (UPOV).

XV: Visegrad Patent Institute (VPI)

XX: recommended to refer to unknown states, other entities or organizations.

- The United Nations Code for Trade and Transport Locations [UNLOCODE] uses the code element "XZ" from the user-assigned range for international waters in accordance with ISO 3166-1 clause 8.1.3:

  "3.2.5 In cases where no ISO 3166 country-code element is available, e.g. installations in international waters or international cooperation zones, the code element "XZ", available for user assignment in accordance with clause 8.1.3 of ISO 3166-1/1997, will be used."

- The World Bank Country API [WORLDBANK] uses the following code elements from the User-assigned range:

  XC: Euro area

  XD: High income

  XE: Heavily indebted poor countries (HIPC)

  XF: International Bank for Reconstruction and Development

  XH: Blend

  XI: International Development Association

  XJ: Latin America and Caribbean (excluding high income)

  XL: Least developed countries: UN classification

  XM: Low income

  XN: Lower middle income

  XO: Low & middle income

  XP: Middle income

XQ: Middle East & North Africa (excluding high income)

XT: Upper middle income

XU: North America

XX: Not classified

XY: Not Classified

- The Interpol Implementation data format for the interchange of fingerprint, facial & scar-mark-tattoo information [INTERPOL] uses code element "ZZ" from the user-assigned range as follows: Destination Agency Identifier "ZZ/ALL" is reserved for transactions which shall be distributed by INTERPOL AFIS to all INTERPOL member states."

- The Certificate Authority Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CABForum] states that if a country is not represented by an official ISO 3166-1 alpha-2 country-code, the CA may specify the user-assigned code element "XX" to indicate that an official code element has not been assigned.

- The UNICODE Common Locale Data Repository (CLDR) [UNICODE] version 37 uses the following code elements from the user-assigned range:

  QO: Outlying Oceania; countries in Oceania that do not have a subcontinent.

  XA: Pseudo-Accents; special code indicating derived testing locale with English + added accents and lengthened.

  XB: Pseudo-Bidi; special code indicating derived testing locale with forced RTL English.

  ZZ: Unknown Region; used in APIs or as a replacement for invalid code.

- The IETF Best Current Practice 47 [BCP-47] contains a section and examples dedicated to private-use subtags, using code elements from the user-assigned range:

  "For example, the region subtags 'AA', 'ZZ', and those in the ranges 'QM'-'QZ' and 'XA'-'XZ' (derived from the ISO 3166-1 alpha-2 private use codes) can be used to form a language tag. A tag such as "zh-Hans-XQ" conveys a great deal of public, interchangeable information about the language material"

- The IETF Proposed Standard "Internationalized Domain Names for Applications" [RFC5890] uses the XN-- prefix. The method that was used to decide on the prefix was explained in an email from the IANA to the IETF IDN Working Group list [XNIDN]:

  "The following steps will be used to select the two-character code:

  The code will be selected from among a subset of the entries on the ISO 3166-1, clause 8.1.3 User-assigned alpha-2 code elements: AA, QM to QZ, XA to XZ, and ZZ. The selection is limited to these codes because of the following:

  The use of ISO 3166-1 User-assigned elements removes the possibility that the code will duplicate a present or future ccTLD code."

5. Private-use top-level Domains

The user-assigned classification of these code elements in the ISO 3166-1 alpha-2 standard allows for the assumption that these code elements will not risk delegation as country-code top-level Domains through future assignments to represent a country or territory. To quote [XNIDN]:

> "The use of ISO 3166-1 User-assigned elements removes the possibility that the code will duplicate a present or future ccTLD code."

Using these code elements as top-level domains for the purpose of private-use TLDs is in line with the intended use of these code elements and follows the many examples of other standards and protocols. Furthermore, they are short and free of any semantic meaning.

This document does not recommend any specific ISO 3166-1 alpha-2 user-assigned code as a private use, but instead proposes that any of them can be used by a network or application for private use. That is, there is no attempt to choose just one of the ISO 3166-1 Alpha-2 user-assigned codes for use as private-use TLDs, just as other organizations use multiple user-assigned codes for many internal purposes.

Note that there may be software that treats labels beginning with XN differently due to the use of the XN- prefix in internationalized domain names [RFC5890].

6. IANA Considerations

This document makes the observation that the policy of assigning ccTLD labels is to align with the ISO-3166-1 alpha-2 standard [RFC1591], which includes user-assigned code elements that will never be assigned to a territory [ISO3166-1]. This is then consistent with existing policies that those user-assigned codes will never be delegated from the DNS root zone and, for that reason, will never give rise to collisions with any future new TLD.

7. Security Considerations

Use of private-use identifiers of any sort almost always results in unexpected collisions in practice. This has repeatedly been shown for private-use addresses, private-use identifiers (such as "x-headers") and private-use names in the DNS. These unexpected collisions can easily have security ramifications that are well beyond what the user understands.

8. Acknowledgements

This document is based on an earlier draft by Ed Lewis. David Conrad, Paul Hoffman, Sion Lloyd, Alain Durand, Jaap Akkerhuis, Kal Feher, Andrew Sullivan, Joe Abley, Petr Spacek, Patrick Mevzek and Kim Davies have played a role.

9. Informative References

[BCP-219] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[BCP-42] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 6895, DOI 10.17487/RFC6895, April 2013, <https://www.rfc-editor.org/info/rfc6895>.

[BCP-47] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <https://www.rfc-editor.org/info/rfc5646>.

[BCP-5] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[BCP-6] Mitchell, J., "Autonomous System (AS) Reservation for Private Use", BCP 6, RFC 6996, DOI 10.17487/RFC6996, July 2013, <https://www.rfc-editor.org/info/rfc6996>.

[CABForum] "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.6.9", March 2020, <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.9.pdf>.

[IANA-Special] "Special-Use Domain Names", n.d., <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml>.

[ICANNISO] "ICANN and the International Organization for Standardization (ISO)", n.d., <https://www.icann.org/resources/pages/icann-iso-3166-2012-05-09-en>.

[ICAO] "International Civil Aviation Organization, Machine Readable Travel Documents, Part 3; Specifications Common to all MRTDs", n.d., <https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf>.

[IMRS] "ICANN Managed Root Server", n.d., <https://www.dns.icann.org/imrs/>.

[INTERPOL] "Interpol Implementation data format for the interchange of fingerprint, facial & smt information", n.d., <https://www.interpol.int/en/How-we-work/Forensics/Fingerprints>.

[ISO3166-1] "ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes", 2013, <https://www.iso.org/standard/63545.html>.

[ISO3901] "Information and documentation -- International Standard Recording Code (ISRC)", n.d., <https://www.iso.org/standard/64817.html>.

[ISO4217] "ISO 4217; Codes for the representation of currencies and funds", n.d., <https://www.iso.org/iso-4217-currency-codes.html>.

[ISO6166] "Securities and related financial instruments -- International securities identification numbering system (ISIN)", n.d., <https://www.iso.org/standard/44811.html>.

[ITHI] "ICANN's Identifier Technology Health Indicator; Queries to frequently leaked strings", n.d., <https://ithi.research.icann.org/graph-m3.html#M332>.

[RFC1591] Postel, J., "Domain Name System Structure and Delegation", RFC 1591, DOI 10.17487/RFC1591, March 1994, <https://www.rfc-editor.org/info/rfc1591>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[STD13] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[STD80] Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, <https://www.rfc-editor.org/info/rfc20>.

[UNICODE] "CLDRv37 - Unicode Common Locale Data Repository version 37", April 2020, <http://cldr.unicode.org/index/downloads/cldr-37>.

[UNLOCODE] "United Nations Code for Trade and Transport Locations; UN/LOCODE Manual", n.d., <https://www.unece.org/fileadmin/DAM/cefact/locode/UNLOCODE_Manual.pdf>.

[WIPO] "World Intellectual Property Organization; Recommended standard on two-letter codes for the representation of states, other entities and intergovernmental organizations.", n.d., <https://www.wipo.int/export/sites/www/standards/en/pdf/03-03-01.pdf>.

[WORLDBANK] "Worldbank API V2 Country API", n.d..

[XNIDN] "Results of IANA Selection of IDNA Prefix", February 2003, <https://psg.com/~randy/lists/iesg/2003/msg01081.html>.

Authors' Addresses

Roy Arends
ICANN

Email: roy.arends@icann.org

Joe Abley
Public Interest Registry
470 Moore Street
London, true N6C 2C2
Canada

Email: jabley@pir.org