Related Domains By DNS
draft-brotman-rdbd-02

Abstract

This document outlines a mechanism by which a DNS domain can publicly document the existence or absence of a relationship with a different domain, called "Related Domains By DNS", or "RDBD".

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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 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 (https://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.
Determining relationships between registered domains can be one of the more difficult investigations on the Internet. It is typical to see something such as "example.com" and "dept-example.com" and be unsure if there is an actual relationship between those two domains, or if one might be an attacker attempting to impersonate the other. In some cases, anecdotal evidence from the DNS or WHOIS/RDAP may be sufficient. However, service providers of various kinds may err on the side of caution and treat one of the domains as untrustworthy or abusive because it is not clear that the two domains are in fact related. This specification provides a way for one domain to explicitly document a relationship with another, utilizing DNS records.
Possible use cases include:

- where a company has websites in different languages, and would like to correlate their ownership more easily, consider "example.de" and "example.ie" registered by regional offices of the same company;

- following an acquisition, a domain holder might want to indicate that example.net is now related to example.com in order to make a later migration easier;

- when doing Internet surveys, we should be able to provide more accurate results if we have information as to which domains are related.

Similarly, a domain may wish to declare that no relationship exists with some other domain, for example "good.example" may want to declare that it is not associated with "g00d.example" if the latter is currently being used in some cousin-domain style attack. In such cases, it is more likely that there can be a larger list of names (compared to the "positive" use-cases) for which there is a desire to disavow a relationship.

It is not a goal of this specification to provide a high-level of assurance as to whether or not two domains are definitely related, nor to provide fine-grained detail about the kind of relationship that may exist between domains.

Using "Related Domains By DNS", or "RDBD", it is possible to declare that two domains are related, or to disavow such a relationship.

We include an optional digital signature mechanism that can somewhat improve the level of assurance with which an RDBD declaration can be handled. This mechanism is partly modelled on how DKIM [RFC6376] handles public keys and signatures - a public key is hosted at the relating-domain (e.g., "example.com") and a reference from the related-domain (e.g., "dept-example.com") contains a signature (verifiable with the "example.com" public key) over the text representation ('A-label') of the two domain names (plus a couple of other inputs).

RDBD is intended to declare or disavow a relationship between registered domains, not individual hostnames. That is to say that the relationship should exist between "example.com" and "dept-example.com", not "foo.example.com" and "bar.dept-example.com" (where those latter two are hosts).
There already exists Vouch By Reference (VBR) [RFC5518], however this only applies to email. RDBD could be a more general purpose solution that could be applied to other use cases, as well as for SMTP transactions.

This document describes the various options, how to create records, and the method of validation, if the option to use digital signatures is chosen.

1.1. Terminology

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

The following terms are used throughout this document:

- Relating-domain: this refers to the domain that is declarating a relationship exists. (This was called the "parent/primary" in -00).

- Related-domain: This refers to the domain that is referenced by the relating-domain, such as "dept-example.com". (This was called the "secondary" in -00.)

2. New Resource Record Types

We define two new RRTYPES, an optional one for the relating-domain (RDBDKEY) to store a public key for when signatures are in use and one for use in related-domains (RDBD).

2.1. RDBDKEY Resource Record Definition

The RDBDKEY record is published at the apex of the relating-domain zone.

The wire and presentation format of the RDBDKEY resource record is identical to the DNSKEY record. [RFC4034]

[[All going well, at some point we’ll be able to say...]] IANA has allocated RR code TBD for the RDBDKEY resource record via Expert Review.

The RDBDKEY RR uses the same registries as DNSKEY for its fields. (This follows the precedent set for CDNSKEY in [RFC7344].)
No special processing is performed by authoritative servers or by resolvers, when serving or resolving. For all practical purposes, RDBDKEY is a regular RR type.

The flags field of RDBDKEY records MUST be zero.  

There can be multiple occurrences of the RDBDKEY resource record in the same zone

2.2. RDBD Resource Record Definition

To declare a relationship exists an RDBD resource record is published at the apex of the related-domain zone.

To disavow a relationship an RDBD resource record is published at the apex of the relating-domain zone.

[All going well, at some point we’ll be able to say...] IANA has allocated RR code TBD for the RDBD resource record via Expert Review.

The RDBD RR is class independent.

The RDBD RR has no special Time to Live (TTL) requirements.

There can be multiple occurrences of the RDBD resource record in the same zone.

The wire format for an RDBD RDATA consists of a two octet rdbd-tag, the relating-domain name(s), and the optional signature fields which are: a two-octet key-tag, a one-octet signature algorithm, and the digital signature bits.

    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 3 3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-----------------------------------------------+-------------------
  |           rdbd-tag            |                               |
  +-----------------------------------------------+-------------------
  /                                            /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /
  /                                           /

We define two possible values for the rdbd-tag in this specification, later specifications can define new rdbd-tag values:
o 0: states that no relationship exists between the domains

o 1: states that some relationship exists between the domains

The relating-domain name(s) field contains either a single domain name, or an HTTPS URL. In the latter case, successfully dereferencing that URL results in a JSON object that contains the list of domain names, such as is shown in the figure below.

```json
[  "example.com",  
  "example.net",  
  "foo.example"
]
```

If an optional signature is included, the sig-alg field MUST contain the signature algorithm used, with the same values used as would be used in an RRSIG. The key-tag MUST match the RDBDKEY RR value for the corresponding public key.

If the optional signature is omitted, then the presentation form of the key-tag, sig-alg and signature fields MAY be omitted. If not omitted then the sig-alg and key-tag fields MUST be zero and the signature field MUST be an empty string. [[Is that the right way to have optional fields in RRs? Not sure.]]

The input to signing ("to-be-signed" data) is the concatenation of the following linefeed-separated (where linefeed has the value ‘0x0a’) lines:

```
relating=<relating-domain name>
related=<related-domain name or URL>
rdbd-tag=<rdbd-tag value>
key-tag=<key-tag>
sig-alg=<sig-alg>
```

The relating-domain and related-domain values MUST be the ‘A-label’ representation of these names.

The trailing "." representing the DNS root MUST NOT be included in the to-be-signed data, so a relating-domain value above might be "example.com" but "example.com." MUST NOT be used as input to signing.
A linefeed MUST be included after the "sig-alg" value in the last line.

[[Presentation syntax and to-be-signed details are very liable to change.]]

See the examples in the Appendix for further details.

3. Directionality and Cardinality

RDBD relationships are uni-directional. If bi-directional relationships exist, then both domains can publish RDBD RRs and optionally sign those.

If one domain has relationships with many others, then the relevant RDBD RRs (and RDBDKEY RRs) can be published to represent those or one RDBD RR can contain an HTTPS URL at which one can provide a list of names.

4. Required Signature Algorithms

Consumers of RDBD RRs MAY support signature verification. They MUST be able to parse/process unsigned or signed RDBD RRs even if they cannot cryptographically verify signatures.

Implementations producing RDBD RRs SHOULD support optional signing of those and production of RDBDKEY RRs.

Implementations of this specification that support signing or verifying signatures MUST support use of RSA with SHA256 (sig-alg==8) with at least 2048 bit RSA keys. \[RFC5702\]

RSA keys SHOULD use a 2048 bit or longer modulus.

Implementations of this specification that support signing or verifying signatures SHOULD support use of Ed25519 (sig-alg==15). \[RFC8080][RFC8032\]

5. Validation

A validated signature is solely meant to be additional evidence that the relevant domains are related, or that one disavows such a relationship. The existence or disavowal of a relationship does not by itself mean that data or services from any domain should be considered as more or less trustworthy.
6. Security Considerations

6.1. Efficacy of signatures

The optional signature mechanism defined here offers no protection against an active attack if both the RDBD and RDBDKEY values are accessed via an untrusted path.

If the RDBDKEY value has been cached, or is otherwise known via some sufficiently secure mechanism, then the RDBD signature does confirm that the holder of the private key (presumably the relating-domain) considered that the relationship, or lack thereof, with a related-domain was real at some point in time.

6.2. DNSSEC

RDBD does not require DNSSEC. Without DNSSEC it is possible for an attacker to falsify DNS query responses for someone investigating a relationship. Conversely, an attacker could delete the response that would normally demonstrate the relationship, causing the investigating party to believe there is no link between the two domains. An attacker could also replay an old RDBD value that is actually no longer published in the DNS by the related-domain.

Deploying signed records with DNSSEC should allow for detection of these kinds of attack.

If the relating-domain has DNSSEC deployed, but the related-domain does not, then the optional signature can (in a sense) extend the DNSSEC chain to cover the RDBD RR in the related-domain’s zone.

If both domains have DNSSEC deployed, and if the relating-domain public key has been cached, then the signature mechanism provides additional protection against active attacks involving a parent of one of the domains. Such attacks may in any case be less likely and detectable in many scenarios as they would be generic attacks against DNSSEC-signing (e.g. if a registry injected a bogus DS for a relating-domain into the registry’s signed zone). If the public key from the relevant RDNDKEY RRs is read from the DNS at the same time as a related RDBD RR, then the signature mechanism provided here may provide little additional value over and above DNSSEC.

6.3. Lookup Loops

It’s conceivable that an attacker could create a loop of relationships, such as a.com->b.com->c.com->a.com or similar. This could cause a resource issue for any automated system. A system SHOULD only perform three lookups from the first domain
(a.com->b.com->c.com->d.com). The related and relating-domains SHOULD attempt to keep links direct and so that only the fewest number of lookups are needed, but it is understood this may not always be possible.

7. IANA Considerations

This document introduces two new DNS RR types, RDBD and RDBDKEY. [[Codepoints for those are not yet allocated by IANA, nor have codepoints been requested so far.]]

[[New rdbd-tag value handling wll need to be defined if we keep that field. Maybe something like: 0-255: RFC required; 256-1023: reserved; 1024-2047: Private use; 2048-65535: FCFS.]]

8. Acknowledgements

Thanks to all who commented on this on the dbound and other lists, in particular to the following who provided comments that caused us to change the draft: Bob Harold, John Levine, Andrew Sullivan, Suzanne Woolf, and Paul Wouters. (We're not implying any of these fine folks actually like this draft btw, but we did change it because of their comments:-) Apologies to anyone we missed, just let us know and we’ll add your name here.

9. Informative References


Appendix A. Examples

This appendix provides examples of RDBD-related values. The following names and other values are used in these examples.

- Relating domain: my.example
- Related domain: my-way.example
- Unrelated domain: my-bad.example
- URL for other related domains: <https://example.com/related-names>
- URL for other unrelated domains: <https://example.com/unrelateds>

The github repo <https://github.com/abrotman/related-domains-by-dns> has a script in sample/mk_samples.sh that generated this appendix.

A.1. Unsigned Examples
### A.2. RSA-signed Example

```bash
# BASH SNIPPET STARTS
# HOWTO generate RSA key pair
$ openssl genrsa -out rsa.private 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
........................................+++........................................++++
e is 65537 (0x010001)
writing RSA key
$ openssl rsa -in rsa.private -out rsa.public -pubout -outform PEM

$ cat rsa.private
---BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA8qpGa2i6076MdGiFVYGgd6UDYyfUN14qHpFxzmrqawUqb8JHM5m8hJlTbKdGDr2aJ5m9sQlaM41hQxpAPuW3mJXYvVOiqtRCB1VTvUCR+Gkah7LUFTS4U8PTc+iF2or2aR7O1L1ITIPnELA2zsB6FwYLsRE8RX89PqeL9U/4xK7jQqSRK88bnRRFs+W7F+iQuA5erHfIZHftq+yzRG8rtrqTNVt0ewkDa2XS2Tn/z0tRVwN UX4M14e/DaE2U0u3kn7HqL0hYBXz/EERUq9+57BURUT/ZQ41RqGJ/+4tv2Gp8mplYdOJaAhzgqky2zGBL1RS+mBFcio9dXBIJywIDAQABAoIBAQDwE7ITtcr6LKy8xmoTKu11NVZBZbKYxU0qUa65n8Q2IWq3jr/jlb85dkmbNQRoL6AvJ+4ifRdQBS6PfCwznZIVkJDsmSyXzB835I3XFiOET3kHvJgCivlgGyVvLo1B9yGbMW1nvjSOhM60A49p9uVROHyB84J3K1EmO/XpmdTPE161CEe+IdYwX3K3w1Mm9C3Sltxrx8gpWhKnpgAG9Z+DA+f406TFTFtUTQe6xCDJk10/uoUGsT62UQqEi0w0wekmB62bzzDdtqu61LqqaKhtGlozXIT7ED+oobp6cAnM1QbV09z7zQezX195yrXt9xZ3odSHNcHnMCR AoGBAP6N00vMmplk760OJ738Twf6fSaL+zkWnmLit4Rwv85LJn96p6xQ0mxwJDmssa7HoC7LwuxhJkhDdbTIlq+oV+Mc4J+FAe5xRX5V7wVmPWTucwvTZXnpr

---END RSA PRIVATE KEY-----
```
# Brotman & Farrell          Expires January 9, 2020         \[Page 12\]

6fU28PqL76feU22G/V2mthgKXOPvYehtceAJAEGbLwQoo1Q7qaZa7Q9i/AoGBAPQL
KSqodzGHJ5iYN+bbbNoqcpqbBbrA7dZstl6WiwQ00U4+kSj3eyyuUEDMz6epXeQD
Ryl1WyoH9yypfLDEP3wF3wp7dqI5yAGzsgospGyGJ0thkJQ3orW+\6Pq19W2aJv2L
QyfODutrjfruIRkgALMoQ8cTRXr1xpx0HpfMOCCX1AoGJ019SPfGgUlhf1lIRxh8e
H91EvTXs2qTDO891i8baW6Ta8xjdiytIAqo/kS9162Ixgew2E2rw8Uo36KfBHI1GKp
INISEN14RDJ9Hxs7rvYD6irU+mtKzcrVwpH2R699MMQt2yn1qco6k9qcyb2kIn4d
z1CrWCwPnJ2JcG2bAIFaHMCgYBX1dD95LAbu/a6dKsPxFAnrYrtj6g7XBDEmuMPY
07nApiW2vN1Vd2FKd4yeJe/\SNdd0/Ji1KIRDQnROxL5JWf9hQEmdfriY4B1UK9v
3/AitNEswi2awL0Dzaoc5QDk3j+01XCOs3d5dWHpirimqiJH51mBh3F+b2q066qrv
EbABLQKBoD0hcsEyIMI0y6o6yKol+iVOZM+a0+64TtKxqUmgHU+qGbdvKy8h9GvxA
kL71hB0BbAyP8obU18R5CMbQq07PITACROu+uYiQ67UREDKjBRt0dcgK0JrRX
kqy4v6LuuFCpS50JQKL6rRfk2XNSjdd12wLuBzjHQd/c/gnm7XRx
-----END RSA PRIVATE KEY-----
$ cat rsa.public
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8qpGa2i6O76MdGiFVYGg
d6UDyFUn14qHpxzmrmugwUb8JHM5m8hjLTbKdGRpZJA5m9sQlaM41hQxpAPw3m
JXYvV0iqtRClBtVtVcR+Gkah7LUTF54U8P7+c7F2or2ArtL70111TIPnEL0AZsbM
6FWyLrsR88BxRQp8Vq5Un4xJ73qSQRR88bnRRFs+W7f+iQa5erHfZfhtq+yzRG
8rtgT7iVhtOewkDa2XS2Tn/07RTvWvNUX4Mi4e/DeUE00u3kn7HqL0hyBzr/EEHug
9+57BURUT/Z410RGj/4+tv2G8mp1yd0JAhzgqky2zGBL1RS+mbFCio9dXBIJ
ywIDAQAB
-----END PUBLIC KEY-----
# To-be-signed data for RSA
$ cat to-be-signed-8.txt
relating=my.example
related=my-way.example
rdbd-tag=1
key-tag=38501
sig-alg=8
# Sign that
$ openssl dgst -sha256 -sign rsa.private -out rsa.sig \
to-be-signed-8.txt
# Hexdump of signature
$ hexdump rsa.sig

00000000 8664 bd57 8cbf a8e1 9182 1b5f a4fc 5eb9
0000010 49b4 fe21 f1c7 8097 ed90 44a5 bcb1 543c
0000020 f784 c190 ed91 2f2b 18ca d3c2 640f 3823
0000030 7f8a e446 d0e8 bd14 6077 0597 6015 a82b
0000040 db72 8677 b1a3 37fa ale8 8109 07ec ff62
0000050 16b8 3859 66de 9929 d2d4 ed99 9ec3 a62b
0000060 4b40 21d6 45f2 d528 1e83 a147 60ce 9b25
0000070 a967 4ba0 3fb5 9b8d dbf3 b070 5b8f 4df8
0000080 f198 6cf1 e6b6 7a6c 1e8c ad22 237f 5440
0000090 7856 caac f96c f87d e79c 4d5c b833 bc03
00000a0 c52e 5603 46a7 59b5 9fe3 fccd 04ee e908
00000b0 71e7 21f8 47ad fea8 40bf 1a4a 9e6b b3d4
00000c0 c6a5 b96e c559 3491 4dfa 91a0 4c0b f3ff
# BASH SNIPPET ENDS

`; ZONE FILE FRAGMENT STARTS

; The RDBDKEY RR for my.example is...

my.example. 3600 IN RDBDKEY 0 3 8 {
  LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0K
  Z2txaGtpRz13MEJBUUVCQFQPQ0RGEFNSU1CQ2dLQ0FRUE4
cXBYTJpNk83Nk1kR21GV11HzwpkN1VEWZWVTmw0UuhWZG6
bXJxYXdvCi4ShhhNNW04aGpMVGLRdScPpKQTvOXRbGFN
NDFcXhwxQVB1VzNtCkpYWZXWT21xeHRSQ0Jsv1R2VUNK0dr
YWg3TFVGVDUOVTvQVctjaUYyb3iyQXJMNO0xTE1UMBvRUww
QVpzYk0KNNZ3WUXzUKu41g0VBxZUw5Ti9VNHhKN2pRcVNS
SzugYm5SUkkZ1k3RiptUXVNWVSY2GJWkmdHEreXpSRwo4
cnRnVE43SHZUT2V3a0RhM1htM1RuL3owdFJWd05WDRNATr1
L0RhrRpVMUuza243SHFMGh5Q1h6LOVFSVxCjkrNTdCVVJV
VC9aUTQxT1JHZ0ovNVCD0jDjHDhtcDF5E9KYUFoemdx43ky
ekdCTDFSUyttQkZDaW85ZFhCSU0KeXdJRERFQUKL0tLS1F
TkQoUFVCTE1DIEtFWS0tLS0tCg== }

; The RDBD RR to be published by my-way.example is...

my-way.example. 3600 IN RDBD 1 my.example 38501 8 {
  ZIXVvb+M4aiCkV8b/KS5XrRJifH8Z2eAKO21RLG8PFSE9DB
  2eErL8oWtMPZCM4in9G5oVQF13YjCFFWatQNdCd4ajsfco3
  6KEJgewHYv+4FpU43ma2U3cme3DnmIKB2qQJ9FKNWDHkeh
  zAlm2epoEui1P9uY819wsIsfj02Y8R9stu2seoweQqI1/1OBU
  Vniy5zfRc58VNM7gOcV7FAranRvVZ45/N04EConncfgh
  rUoe/C9apRrntSzGsaW1nFT6TaCRC0z/82dkeitJfmhT
  44W+Fmv+moB9EcvCGb66xZR1Y+cfJ1RePmhbeUDxinzD3n
  NxKcA== }

; ZONE FILE FRAGMENT ENDS

A.3. Ed25519-signed Example
# BASH SNIPPET STARTS
# HOWTO generate an Ed25519 key pair...
$ ./ed25519-signer.py -s rdbd-example0001rdbd-example0002 \ 
   -r my.example -d my-way.example
private:b'726462642d6578616d7066530303031726462642d6578616d
7066530303032'
public:b'353fc3e1166c91f0af65d6c26fd441fb7df9671a23a746bb3e
86be8d35b648'
b64pubkey: NT/DHhFoyR8K911sJv1EH7fflnGiOnRrs+yGvo01tkg=
keyid: 35988
to-be-signed:|relating=my.example
related=my-way.example
rdbd-tag=1
key-tag=35988
sig-alg=15
|  
sig:b'64bc444ce759fb9435fe9c1875eb241c4ec6d0995cd8138a372782
32fc8e79f53cb8f88059f6040054c61be8cfd73fd44521f73994628fc7c3
0135fa929ab0f'
# hex dump of Ed25519 private
$ hexdump ed25519.priv
0000000 6472 6462 652d 6178 7066530303031726462642d6578616d
7066530303032
0000010 6472 6462 652d 6178 7066530303031726462642d6578616d
7066530303032
0000020
# hex dump of Ed25519 public
$ hexdump ed25519.pub
0000000 3f35 1ec3 6811 1fc9 f60a 6c5d fd26 1f44
0000010 dbf7 7196 3aa2 6b74 ecb3 be86 358d 48b6
0000020
# hex dump of Ed25519 signature
$ hexdump ed25519.sig
0000000 bc64 4c44 59e7 94fb fe35 189c eb75 1c24
0000010 c64e 99d0 d85c 8a13 2737 3282 8efc f579
0000020 b83c 80f8 f659 0004 c654 e81b d7cf d43f
0000030 2145 39f7 6294 c78f 01c3 fa35 9a92 0fb0
0000040
# BASH SNIPPET ENDS

; ZONE FILE FRAGMENT STARTS
; The RDBDKEY RR for my.example is...
my.example. 3600 IN RDBDKEY 0 3 15 (NT/DHhFoyR8K911sJv1EH7fflnGiOnRrs+yGvo01tkg=)
; The RDBD RR to be published by my-way.example is...
my-way.example. 3600 IN RDBD 1 my.example 35988 15 (ZLxETOdZ+5Q1/pwYdeskHE7G0J1c2BOKNyeCMvyOefU8uPiA
WfYEAPTGG+jP1z/URSH3OZRij8fDATX6kpqwDw==)
; ZONE FILE FRAGMENT ENDS
Appendix B. Ed25519 Signing Code

Since OpenSSL does not yet support Ed25519 signing via its command line tool, we generate our example using the python script below, which is called as "ed25519-signer.py" above. This uses the python library from Appendix A of [RFC8032].

```python
#!/usr/bin/env python3
# CODE_BEGINS
import argparse, sys, binascii
from eddsa2 import Ed25519
# from https://gist.github.com/wido/4c6288b2f5ba6d16f937dca3fc2cb4a
def calc_keyid(flags, protocol, algorithm, dnskey):
    st=struct.pack('!HBB', int(flags), int(protocol), int(algorithm))
    st+=base64.b64decode(dnskey)
    cnt = 0
    for idx in range(len(st)):
        s = struct.unpack('B', st[idx:idx+1])[0]
        if (idx % 2) == 0:
            cnt += s << 8
        else:
            cnt += s
    return ((cnt & 0xFFFF) + (cnt >> 16)) & 0xFFFF

def main():
    parser=argparse.ArgumentParser(description='Ed25519 signing')
    parser.add_argument('-s','--secret', dest='secret', help='secret key')
    parser.add_argument('-r','--relating', dest='relating', help='relating domain')
    parser.add_argument('-d','--related', dest='related', help='related domain')
    parser.add_argument('-n','--negative', dest='negative', help='negative assertion')
    args=parser.parse_args()

    if args.secret is None:
        print("You do need a secret... - exiting")
        sys.exit(1)
    # secret has to be 32 octets funny enough:-)
    # e.g. secret="rdbd-example0001rdbd-example0002".encode('utf-8')
    if len(args.secret)!=32:
        print("Secret has to be 32 octets... - exiting")
        sys.exit(1)
    if args.relating is None:
        print("You do need a relating domain... - exiting")
```

Brotman & Farrell        Expires January 9, 2020               [Page 15]
sys.exit(1)
if args.related is None:
    print("You do need a related domain... - exiting")
sys.exit(1)
secret=args.secret.encode('utf-8')
privkey,pubkey = Ed25519.keygen(secret)
print("private:"+ str(binascii.hexlify(privkey)))
print("public:"+ str(binascii.hexlify(pubkey)))
b64pubkey=binascii.b2a_base64(pubkey).rstrip().decode("utf-8")
print("b64pubkey: " + b64pubkey)
keyid=calc_keyid("0","3","15",b64pubkey)
print("keyid: " + str(keyid))

rdbdtag="1"
if args.negative:
    rdbdtag="0"

tbs="relating="+args.relating+"\nrelated="+\n    args.related+"\nrdbd-tag="+rdbdtag+"\nkey-tag="+str(keyid)+"\nsig-alg=15\n"
print("to-be-signed:"+ str(tbs)+")")

with open("ed25519.priv", "wb") as privf:
    privf.write(privkey)
with open("ed25519.pub","wb") as pubf:
    pubf.write(pubkey)
with open("to-be-signed-15.txt","wb") as tbsf:
    tbsf.write(tbs.encode('utf-8'))

msg=tbs.encode('utf-8')
signature = Ed25519.sign(privkey, pubkey, msg)
print("sig:"+ str(binascii.hexlify(signature)))
with open("ed25519.sig", "wb") as sigf:
    sigf.write(signature)
return

if __name__ == "__main__":
    main()

# CODE_ENDS

Appendix C. Changes and Open Issues

[[RFC editor: please delete this appendix ]]
C.1. Changes from -01 to -02

- Added negative assertions based on IETF104 feedback
- Added URL option based on IETF104 feedback
- Made sample generation script
- Typo fixes etc.

C.2. Changes from -00 to -01

- Changed from primary/secondary to relating/related (better suggestions are still welcome)
- Moved away from abuse of TXT RRs
- We now specify optional DNSSEC-like signatures (we’d be fine with moving back to a more DKIM-like mechanism, but wanted to see how this looked)
- Added Ed25519 option
- Re-worked and extended examples

C.3. Open Issues

Current open github issues include:

- #5: specify input for signing more precisely - e.g. is there a CR or NULL or not
- #6: what, if anything, does rdbd for example.com mean for foo.example.com?

These can be seen at: <https://github.com/abrotman/related-domains-by-dns/issues>

Authors’ Addresses

Alex Brotman
Comcast, Inc

Email: alex_brotman@comcast.com
Stephen Farrell
Trinity College Dublin

Email: stephen.farrell@cs.tcd.ie