Abstract

This document describes 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 March 21, 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.
1. Introduction

Determining relationships between DNS 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 if it is not clear that the two domains are in fact related. This specification provides a way for one domain to explicitly document, or disavow, relationships with other domains, utilizing DNS records.

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 kinds of relationships
that may exist between domains. However, the mechanism defined here is extensible in a way that should allow use-cases calling for such declarations to be handled later.

1.1. Use-Cases

The use cases for this include:

- where an organisation has names below different ccTLDs, and would like to allow others 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, or are not, related;

- a domain holder 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 which case, 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.

[[Discussion of this draft is taking place on the dnsop@ietf.org mailing list. Previously, discussion was on the dbound@ietf.org list. There’s a github repo for this draft at <https://github.com/abrotman/related-domains-by-dns> - issues and PRs are welcome there.]]

1.2. 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 declaring 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 a resource record type (RDBD) that can declare, or disavow, a relationship. RDBD also includes 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., "club.example.com"), using an RDBDKEY resource record, and the RDBD record of the Related-domain (e.g., "member.example.com") can contain a signature (verifiable with the "club.example.com" public key) over the text representation (‘A-label’) of the two names (plus a couple of other inputs).

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. [[In the meantime we’re experimenting using 0xffa8, which is decimal 65448, from the experimental RR code range, for the RDBDKEY resource record.]]

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. [[Is that correct/ok?]]

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. [[In the meantime we’re experimenting using 0xffa3, which is decimal 65443, from the experimental RR code range, for the RDBD resource record.]]

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.

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

The wire format for an RDBD RDATA consists of a two octet rdbd-tag, a domain name or URL, 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 2 2 2 2 2 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
  +----------------------------------------+
<table>
<thead>
<tr>
<th>rdbd-tag</th>
</tr>
</thead>
</table>
  /                               |
  /--------------------------------|
  / domain name or URL             |
  /--------------------------------|
  / key-tag                        |
  /--------------------------------|
  / sig-alg                        |
  /--------------------------------|
  / signature                      |
  /--------------------------------|

We define two possible values for the rdbd-tag in this specification, later specifications can define new rdbd-tag values:

- 0: states that no relationship exists between the domains
- 1: states that some relationship exists between the domains
The domain name field contains either a single domain name, or an HTTPS URL. In the latter case, successfully de-referencing that URL is expected to result in a JSON object that contains a list of domain names, such as is shown in the figure below.

```
[  
  "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, and is calculated as defined in [RFC4034] appendix B.

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 presentation syntax for RRs?]]

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.

The rdbd-tag and key-tag and sig-alg fields MUST be in decimal with leading zeros omitted.

A linefeed MUST be included after the "sig-alg" value in the last line.
3. RDBD processing

- If multiple RDBD records exist with conflicting "rdbd-tag" values, those RDBD records SHOULD be ignored.

- If an RDBD record has an invalid or undocumented "rdbd-tag", that RDBD record SHOULD be ignored.

- The document being referenced by a URL within an RDBD record MUST be a well-formed JSON [RFC8259] document. If the document does not validate as a JSON document, the contents of the document SHOULD be ignored. There is no defined maximum size for these documents, but a referring site ought be considerate of the retrieving entity’s resources.

- When retrieving the document via HTTPS, the certificate presented MUST properly validate. If the certificate fails to validate, the retrieving entity SHOULD ignore the contents of the file located at that resource.

- Normal HTTP processing rules apply when de-referencing a URL found in an RDBD record, for example, a site may employ HTTP redirection.

- 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 MUST 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]
A validated signature is solely meant to be additional evidence that the relevant domains are related, or that one disavows such a relationship.

4. Use-cases for Signatures

[[The signature mechanism is pretty complex, relative to anything else here, so it might be considered as an at-risk feature.]]

We see two possibly interesting use-cases for the signature mechanism defined here. They are not mutually exclusive.

4.1. Many-to-one Use-Case

If a bi-directional relationship exists between one Relating-domain and many Related-domains and the signature scheme is not used, then making the many required changes to the Relating-domain zone could be onerous. Instead, the signature mechanism allows one to publish a stable value (the RDBDKEY) once in the Relating-domain. Each Related-domain can then also publish a stable value (the RDBD RR with a signature) where the signature provides confirmation that both domains are involved in declaring the relationship.

This scenario also makes sense if the relationship (represented by the rdbd-tag) between the domains is inherently directional, for example, if the relationship between the Related-domains and Relating-domain is akin to a membership relationship.

4.2. Extending DNSSEC

If the Relating-domain and Related-domain zones are both DNSSEC-signed, then the signature mechanism defined here adds almost no value and so is unlikely to be worth deploying in that it provides no additional cryptographic security (though the many-to-one advantage could still apply). If neither zone is DNSSEC-signed, then again, there may be little value in deploying RDBD signatures.

The minimal value that remains in either such case, is that if a client has acquired and cached RDBDKEY values in some secure manner, then the RDBD signatures do offer some benefit. However, at this point it seems fairly unlikely that RDBDKEY values will be acquired and cached via some secure out-of-band mechanisms, so we do not expect much deployment of RDBD signatures in either the full-DNSSEC or no-DNSSEC cases.

However, where the Relating-domain’s zone is DNSSEC-signed, but the Related-domain’s zone is not DNSSEC signed, then the RDBD signatures...
do provide value, in essence by extending DNSSEC "sideways" to the Related-domain. The figure below illustrates this situation.

Extending DNSSEC use-case for RDBD signatures

5. Security Considerations

5.1. 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.

5.2. 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.

5.3. Lookup Loops

A bad actor could create a loop of relationships, such as a.example->b.example->c.example->a.example or similar. Automated systems SHOULD protect against such loops. For example, only performing a configured number of lookups from the first domain. Publishers of RDBD records 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.
6. 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 will 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. It will also likely be useful to define a string representation for each registered rdbd-tag value, e.g. perhaps "UNRELATED" for rdbd-tag value 0, and "RELATED" for rdbd-tag value 1, so that tools displaying RDBD information can be consistent.])

7. 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, Pete Resnick, Andrew Sullivan, Tim Wisinski, Suzanne Woolf, Joe St. Sauver, 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.

8. References

8.1. Normative References


8.2. Informative References


Appendix A. Implementation (and Toy Deployment:-) Status

[[Note to RFC-editor: according to RFC 7942, sections such as this one ought not be part of the final RFC. We still dislike that idea, but whatever;-)]

We are not aware of any independent implementations so far. One of the authors has a github repo at <https://github.com/sftcd/rdbd-deebeedeerrr> with scripts that allow one to produce zone file fragments and signatures for a set of domains. There is also a wrapper script for the dig tool that provides a nicer view of RDBD and RDBDKEY records, and that verifies signatures. See the README there for details.

In terms of deployments, we used the above for a "toy" deployment in the tolerantnetworks.ie domain and other related domains that one can determine by following the relevant trail:-)

Appendix B. Examples

These examples have been generated using the proof-of-concept implementation mentioned above. These are intended for interop, not for beauty:-) The dig wrapper script referred to above produces more readable output, shown further below..

The following names and other values are used in these examples.
o Relating domain: my.example

o Related domain: my-way.example

o Unrelated domain: my-bad.example

o URL for other related domains: <https://my.example/related-names>

o URL for other unrelated domains: <https://my.example/unrelateds>

my.example zone file fragments:

```
my.example.     3600 IN TYPE65448 \# 298 ( 0000030830820122300d06092a864886f70d010101050
00382010f003082010a0282010100bb3b09979b3c4e61
0f231dafbd8295d56d9475eba8df1cff49b08b99a768
15e660c243b8ce7175cc9857be00847cff865ca81e56a
f0ec813a43787902e8b2560b64016c4c8e64262b7b8e
ae2e6f735e1186237fff49110227b69fbcefa1cfddff7f
df052f250871bb03be114493a8e29a95d04b50b9e9b9b5
8e40e70381384c159d02d781e6837791c2ead0c547e7f
fb0aaa19hb2aeef259c42273a69af4f22c7439972d3052d
4a581895ae203115963689044b4cbbdb6cf90ff1866630
593aad625772e6f540bd93801c5781fd74481fbb6399
f745b4525c767e3fb4a4d919e265d541f6ehee95d0b9e1
15bd4749a3a9748e2d8745466629fa6882d36e83cbae8
30203010001
)

my.example.     3600 IN TYPE65443 \# 85 ( 0001066d792d776179076578616d706c650039820f039
b08e9d5a8e057a87c6e7ddb92a680b7a2e69baef46404
b3bc9fcd93f4fe261bda56c107dba2d672255a86a771f
cc3cea0f12cdd1b302f20b2234de8610e03
)

my.example.     3600 IN TYPE65443 \# 18 ( 000006d792d626164076578616d706c6500
)

my.example.     3600 IN TYPE65443 \# 39 ( 00012368747470733a2f2f6d792d7761792e6578616d7
06c652f6d797374756662e6a736f6e00
)

my.example.     3600 IN TYPE65443 \# 42 ( 00002668747470733a2f2f6d792d7761792e6578616d7
06c652f6e6f746d797374756662e6a736f6e00
)
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAuzsJl5s8TmEPix2vvYKV1bbZR166jfHP9JsUu2p2qV5mDCQ7
jOCXMMFeAiR8/4zEC5Bw5r7BgpDeHkc6IWC2QBBeyOZCye46ulM9xXhGGI3
//SREC7JafVo+hz933/ fBS81CHG7A74RR0o4pqV0EtQuembWOQOCqThMFZ0Cl4
Hmq3ErwquXUnf/7/CqGysq7ywQcic6aa9P1sdDmXLTS1KB1v4gMRWNOkES0y7
2z2s5D/GGZjbOqiiV3lm9UC9k4AcV4H10S8+B7Y5n3RbRSHXH+P7Sk2RniZdBVB9r
7pQXueVvUdJo610jihHRUZKfpmgtNug8uugwIDAQABoIBAfIsJuwkBGJGjocb2
4CltGtsVorMu/E0pIdDr+F2MSKhdhD/ BM/ /3drWVagaJGcMKzWkipXYptToisUs1vd
cGJszJzeWrh96nEIG/XgIh/reltuDBQ39hNcOCnh2szWXb+FSDqEnqacM6RFBw
pw0d1K5FTi2h9wDIkupF988y9h4OzV1k591Dq0ZKAKnxoyY20xiq1aU6NeHrs2
Sv7ow5CErKm3DZqvtccqs+wB1m3is5LsPGKexDZfXDOQ1e7hJFbXKUw+2REF8hzc
bCfa3A5Xyo7LdgGRD0Z1zQQA+iiz5Cnpb35gdOv+giptwndrn81c8U1zlf1f47T
a0xh2YEcgYEA4uV/VQB4UX4NNX8g3womG/jZOMowVxk8d8dRhBy4s0c+atGy3ztp
SOprBqrkjcFE831b596MOE11y1gpmK7k5nI2ICmuStnLoj27a95QVznwbyA6a
g3cIAz/10HcexLz8edjcwTJv1XNE9518SbkU0Ebw20Y5jZsHUI4OMCGyAe0zVt
m3PrU5/JW1GqmRhdA7PyfB9E8sq5mIXiaT6mp0XlyMn2uLMFBMC3iuxNayJqgZI
Gg3XVC1cb4vvrVDrkxY5aTDmizvVvF0MletBlyjCwWHaOGq14hxwhvENyCyVCjs
T0WSHg8uuumAH371+2HbKReEhlHR1y0h0m2C8ECyE4A4Cc5pSNnRj19h2Wztc
eGbu81qVPNmQ51nQMe8g1LTz5Lj0mSK11h4N6Ze0eKyrJACzJkF2fewfPaeCOB3
/bnMqJHDSuclTXXtf2jq0HzdAIR87FcnJ3jegTil1R0Ik/k/yMrUGOncNa1u+85DB
7Xsy3f/LZoAESasJCWay6cGcYAgpc5Bs8WVo5f5K/LMVzUH+oUhAf801hI8dg
G15m/c37EH0o+aVVCb8iYdgLPlpwOig4aOCXb19A12j6dAbehsgpzyLx5sjmFYBt
1DgnsSrAfCFy0MmH3aN28VRCXjuxoAemgQaTQHyx9sNTcQ÷dB/ivVxrCl7q
ziaNQKBq6C9MEcVh/bYjYV6roc52YAA6A4CYDHaNw040Q0ckSgWf3Fen7vw
b2qg7zLOCXZ2Z+6HjeJMNCG/eE2KVNO0kpe4KGOxChD3pYrrLsLCNRX8x8SyOIt
e3elKArigiXcrsPBbn7nakUa72307Hb31c0GMYf9znN+qWda+3g==
-----END RSA PRIVATE KEY-----

my-way.example zone file fragments:

my.example private key:
my-way.example. 3600 IN TYPE65448 \# 36 (0000030f6d5a2d3caf0d740e139d36a0e52325c4e078e7623f19be3b872367dc8027ef42)

my-way.example. 3600 IN TYPE65443 \# 273 (0001026d79076578616d706c65003e6c088d887950e26305a59bbe63263b65d34e11656968497500cbebf7af12be14d173d7368e24da54258c851456d3c2d94437692879d1d2b5d3f0acf1e3de6ebb345f8c31f209af6fd7f27313804fc79db421231126e3e42115ce51a81d2619ed221afea2b64d1d9ffbef0bd4786fbe5f42c75951ae645078db7a5a88ed3173d4a209734f49a23a0920ce38ed44011d784e47cf7658c313cf01349c80b936b17fca3542f32aff956e808c2520736a917df648e4e5f2eea5de994ce90dbaf6d5051a4e0934da4a9f6ff01ef5df98d3b4da52b12ea3b8e7ebabcfc6d7a0a170dc1284753e3e6b039f8a32ce707312ea5b02180072b517a6056db6e47f8dd5240ab1874646)

my-way.example private key:

0000000 5f24 3132 d0a0 4cc4 0a77 4cb6 e834 16db
0000020 05b0 faf7 ca27 16b6 0ae7 e177 d3f9 db5f
0000040

Appendix C. Possible dig output...

Below we show the output that a modified dig tool might display for the my.example assertions above.
$ dig RDBD my.example

; <<>> DiG 9.11.5-P1-1ubuntu2.5-Ubuntu <<>> RDBD my.example
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4289
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: e69085d4b9a18cca63ae96035d7bc0aa96580e0d6255c122 (good)
;; QUESTION SECTION:
;;my.example. IN RDBD

;; ANSWER SECTION:
my.example. 3600 IN RDBD RELATED may-way.example Sig: good
  KeyId: 50885 Alg: 15 Sig: UIi04agb...
my.example. 3600 IN RDBD UNRELATED my-bad.example
my.example. 3600 IN RDBD RELATED https://my-way.example/mystuff.json
my.example. 3600 IN RDBD UNRELATED https://my-way.example/notmine.json

;; Query time: 721 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Sep 13 17:15:38 IST 2019
;; MSG SIZE rcvd: 600

Appendix D. Changes and Open Issues

[[RFC editor: please delete this appendix ]]

D.1. Changes from -02 to -03

- Incorporated feedback/comments from IETF-105
- Suggest list dicussion move to dnsop@ietf.org
- Adopted some experimental RRCODE values
- Fixed normative vs. informative refs
- Changed the examples to use the PoC implementation.
- Restructured text a lot
D.2. 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.

D.3. 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

Authors’ Addresses

Alex Brotman
Comcast, Inc

Email: alex_brotman@comcast.com

Stephen Farrell
Trinity College Dublin

Email: stephen.farrell@cs.tcd.ie