Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 29, 2019

A. Brotman
Comcast, Inc
S. Farrell
Trinity College Dublin

February 25, 2019

Related Domains By DNS
draft-brotman-rdbd-00

Abstract

This document outlines a mechanism by which a registered domain can create a relationship to a different registered 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 http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 29, 2019.

Table of Contents

1. Introduction 2
1.1. Terminology 3
2. DNS Record for Secondary Domain 3
3. DNS Record for Parent Domain 4
4. Validation 5
5. Steps to validate 5
6. Security Considerations 5
6.1. DNSSEC 5
6.2. Lookup Loops 5
7. References 6
7.1. Normative References 6
7.2. Informative References 6
Appendix A. Creating a Signature for the Secondary Domain . . . 6
A.1. Sample Signature 6
Authors' Addresses 8

1. Introduction

[[There's a github repo for this -- issues and PRs are welcome there. <https://github.com/abrotman/related-domains-by-dns>

Current issues include:

- #1: use TXT or new RR? (ATB: new RR, but TXT for now)
- #2: stick with a 1:n thing or design for m:n relationshops (ATB: m:n is possible (I believe) as it stands, using selectors)
- #3: include an indicator for the kind of relationship or not?
- #4: "h=" is wrong for a signature, but "s=" is selector, bikeshed later
- #5: specify input for signing more precisely - e.g. is there a CR or NULL or not]]

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 places such as DNS or WHOIS/RDAP may suffice. However, service providers of various kinds may err on the side of caution and mark the secondary domain being untrustworthy or abusive because it is not clear that they are in fact related. Another possible use case could be where a company has

two websites in different languages, and would like to correlate their ownership more easily, consider "example.at" and "example.de" registered by regional offices of the same company. A third example could be an acquisition where both domains continue to operate.

Using "Related Domains By DNS", or "RDBD", it is possible to indicate that the secondary domain is related to the primary domain. This mechanism is modelled on how DKIM [RFC6376] handles public keys and signatures - a public key is hosted at the parent domain ("example.com") and a reference from the secondary domain ("dept-example.com") contains a signature (verifiable with the "example.com" public key) over the text representation ('A-label') of the primmary and secondary domain names.

RDBD is intended to demonstrate 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".

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 a record, and the method of validation.

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:

- Parent domain: This refers to the domain that is to be referenced, such as "example.com".
- Secondary domain: This will refer to the domain that references the parent domain, such as "dept-example.com".

2. DNS Record for Secondary Domain

There are a few options when publishing the reference to the parent domain.

- "v": Version string, which should be set to "RDBD1".

- "d": The Parent Domain. This should be in the form of "example.com".

- "s": The selector, which is the same as defined in [RFC6376] and used to denote which published public key should be used.

- "h": The base64 encoded signature over the primary and secondary domain namess, created using the private key.

A sample TXT record for "dept-example.com" would appear as:

"v=RDBD1;s=2018a;d=example.com;
h=TkKgbCV7xXWYES+I5y8KRvgQet7SOLUYTbJtjVyb2/H/
phI4EcalpxhDfADPgCRwxASztR12BMq0 MLWJZZYxN1zuBE3joFED7EHRoDlFQti/
GtRFg9lyOSLac58dyty3rdU2oLDSubbk21YYZZV7VsUh OqbGxrhe6LdY0f59aw7cGg2R
+YIX0dW9z+I3cOcZKtdlfea42AS6sL4vJBy+ytWmfJC62wDL5IT3 HDmWVEmZg7GcSbT0
62zQBUX0Xo3sDOquXyA2qzat4Gbq3FJeSTFEc3UQipHFBohb0qIkbWv2IeHC
m2nYjnaCi8P9o3y2nBn1rfzuHB2ctPnnTqK+eg=="

The input to signing is:

s=dept-example.com&p=example.com

Where:

s: The secondary domain p: The primary domain

For internationalised domain names, the punycode ('A-label') version is the input to signing.

3. DNS Record for Parent Domain

- "v": Version string, which should be set to "RDBD1".

- "s": The selector, which is the same as defined in [RFC6376] and is a string used to denote a specific public key published by the Parent Domain.

- "k": The public key published for this selector, encoded using base64.

A sample TXT record for the parent domain of "example.com":

"v=RDBD1;s=2018a;
k=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2LNjBAdNAtZOMdd3hl
emZF8a0onOcEo5g1KWnKzryDCfH4LZkXOPzAJvz4yKMHW5ykOz9OzGL01GMl8ns8
Ly9ztBXc4obY5wnQpl4nbvOdf6vyLy7Gqgp+dj6RrycSYJdLitiYapHwRyuKmERl
QL6MDWLU9ZSWlqskzLVPgwqtT80xchU65HipKkr2luSAySZyyNEf58pRea3D3pBk

Ly5hCDhr2+6GF2q9lJ9qMopd2P/ZXxHkvzl3TFtX6GjP5LTsb2dy3tED7vbf/EyQ
fVwrs4495a8OUkOBy7V4YkgKbFYSSkGPmhWoPbV7hCQjEAURWLM9J7EUou3U1WIq
Tj1QIDAQAB"

And the TXT location for this record would be:

"2018a._rdbd.example.com"

This is constructed by using the selector (s=) in the secondary domain's reference to the first domain. The absence of the record in this location MUST be considered a failure to validate, and a failure to establish the relationship.

4. Validation

The validated signature is solely meant to be evidence that the two domains are related. The existence of this relationship is not meant to state that the data from either domain should be considered as more trustworthy.

5. Steps to validate

A validating system should use the combination of the Secondary Domain name and public key from the Parent Domain record to be able to verify the signature that is stored in the record for the Secondary Domain. This is demonstrated in the appendix.

6. Security Considerations

6.1. DNSSEC

RDND does not require DNSSEC. It could be 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.

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

6.2. Lookup Loops

It's conceivable that an attacker could create a loop of lookups, 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 original domain (a.com->b.com->c.com->d.com). The Secondary and Parent SHOULD

attempt to keep the link direct and limited to a single lookup, but it is understood this may not always be possible.

7. References

7.1. Normative References

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

7.2. Informative References

[RFC5518] Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference", RFC 5518, DOI 10.17487/RFC5518, April 2009, <https://www.rfc-editor.org/info/rfc5518>.

Appendix A. Creating a Signature for the Secondary Domain

Appendix C of [RFC6376] has some reference material on how to create a set of keys for use in this type of use case. The key length is recommended to be at least 2048 bits instead of the 1024 recommended in that appendix.

A.1. Sample Signature

Creation of keys:

openssl genrsa -out rsa.private 2048 openssl rsa -in rsa.private -out rsa.public -pubout -outform PEM

Keys in use:

rsa.private: -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2LNjBAdNAtZOMdd3hlemZF8a0onOcEo5g1KWnKzryDCfH4LZ
kXOPzAJvz4yKMHW5ykOz9OzGL01GMl8ns8Ly9ztBXc4obY5wnQpl4nbvOdf6vyLy
7Gqgp+dj6RrycSYJdLitiYapHwRyuKmERlQL6MDWLU9ZSWlqskzLVPgwqtT80xch
U65HipKkr2luSAySZyyNEf58pRea3D3pBkLy5hCDhr2+6GF2q9lJ9qMopd2P/ZXx
Hkvzl3TFtX6GjP5LTsb2dy3tED7vbf/EyQfVwrs4495a8OUkOBy7V4YkgKbFYSSk
GPmhWoPbV7hCQjEAURWLM9J7EUou3U1WIqTj1QIDAQABAoIBAH/eAgwrfq6w4/0X
Bgk4iQ9q6vnWpQCvW5Z40jRq+MnsnshKPrVL+krIGU/fvt7vaIzIPFTGrf7VWxl3
+oZg/1sRFPYUItjaluqjaxEhWvHH1saYCb2lAV1x9QtkgjBv4F6GZqfi1MJfro32
QP36s/hIaVjdHHNsB7BkDgr6VEVIR5y2PmW4aLjHCiqsyDIUM4zRcl4exzw+rst1
z2seOhhJrnYdc+VnkEg5GKENldZ3tZoY3je/OsfNJtKjpArPRqkP1qve3h3uD+PK
obZ7BM+xok29Fxf6AgC99eDr9BatTa/a8q7NYMkVRLq/JdOF1XUuDDNd3r93Ae4n
54qqucECgYEA/Xuct8ALG2/6Kd4Lmm9i055LVxdwB+1wG1JNE1IB+OI+6B8W49po vK/
fFVHMEV2BoRr4EB58Xxa+oICBImIzTUQXYQnMbDzL2N+X3FrkDSGCPZQy7GzD

```
wFdpY3ceNShou1bRt4/hPWLLI35ZXM3yqBJeGhbTUmYVdWrkXTNo2wUCgYEA2tpE
+bg9iIYUJAg/CEpdWn+8ZxhRnBDziN88Grli+arSWaMWE809GyPaeiplbwywnXRb
vliskE43CcgstnhRKY8dWB2AQnRESvsJKO8rw/ONSxlWTpFc78xxmmNSvOBs4Srv
quMc6HTMaetCM5/l0PddCY3/rls9FTESf36RXpECgYEA5AF6mHYwB4AT3/ERMtsa
ZAuw7Sfx58+V1Z2UItrTV1H7D8RXTKE7MO5plb2796rKXWXq2GTzrnzA/5JXldwL
FWc4OFsd/AY7vlpxOQ6wr3cCte1GWRAEjFCURZnyHBK7Ejgn8BuFmTfyTXzrWOUP
bksHRiRd9XJJvxJlU8hYexkCgYBhM9i24THTVVnUtyTn1b+o1lsjnxWAL7c674uO
gxCGu2w6C8leeiXNzBrZb8Mlk4lOJcQpwtDCNzsSySmy0bWas8ngvRmeam16sAzd
dX0Gx0HWPSasNrwEddVvMPYqlbNGPv+78quAQ4AW+zqoGzjDm1pjSAJrunJi2yzQ
G7MNQQKBgCZktECUg2xr8vgVTB586sB7PiHp2j8Wabxh+dMiNUEB7qg4HZdzh8XA
JXnJnZVQWBL0s10yPg9oITWVBcZ3MqgOqsN1QamN9KjzA46ILtpWptz2q3Nw2Tkl
m7RBP9R9gM9mnl9/azK7Y5uj11/O3cNJLEIWcraKqydPfvxNyEtP -----END RSA
PRIVATE KEY-----

rsa.public: -----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2LNjBAdNAtZOMdd3hlem
ZF8a0onOcEo5g1KWnKzryDCfH4LZkXOPzAJvz4yKMHW5ykOz9OzGL01GMl8ns8Ly
9ztBXc4obY5wnQpl4nbvOdf6vyLy7Gqgp+dj6RrycSYJdLitiYapHwRyuKmERlQL
6MDWLU9ZSWlqskzLVPgwqtT80xchU65HipKkr2luSAySZyyNEf58pRea3D3pBkLy
5hCDhr2+6GF2q9lJ9qMopd2P/ZXxHkvzl3TFtX6GjP5LTsb2dy3tED7vbf/EyQfV
wrs4495a8OUkOBy7V4YkgKbFYSSkGPmhWoPbV7hCQjEAURWLM9J7EUou3U1WIqTj
1QIDAQAB -----END PUBLIC KEY-----

File containing domain, domain.txt:

$ cat domain.txt

s=foo-example.com&p=example.com

$ openssl dgst -sha256 -sign rsa.private -out foo.sign domain.txt

$ base64 foo.sign TkKgbCV7xXWYES+I5y8KRvgQet7SOLUYTbJtjVyb2/H/
phI4EcalpxhDfADPgCRwxASztR12BMq0 MLWJZZYxN1zuBE3joFED7EHRoDlFQti/
GtRFg9lyOSLac58dyty3rdU2oLDSubbk21YYZZV7VsUh OqbGxrhe6LdY0f59aw7cGg2R
+YIX0dW9z+I3cOcZKtdlfea42AS6sL4vJBy+ytWmfJC62wDL5IT3 HDmWVEmZg7GcSbT0
62zQBUX0Xo3sDOquXyA2qzat4Gbq3FJeSTFEc3UQipHFBohb0qIkbWv2IeHC
m2nYjnaCi8P9o3y2nBn1rfzuHB2ctPnnTqK+eg==

The published record would be: "v=RDBD1;s=2018a;d=example.com;
h=TkKgbCV7xXWYES+I5y8KRvgQet7SOLUYTbJtjVyb2/H/
phI4EcalpxhDfADPgCRwxASztR12BMq0 MLWJZZYxN1zuBE3joFED7EHRoDlFQti/
GtRFg9lyOSLac58dyty3rdU2oLDSubbk21YYZZV7VsUh OqbGxrhe6LdY0f59aw7cGg2R
+YIX0dW9z+I3cOcZKtdlfea42AS6sL4vJBy+ytWmfJC62wDL5IT3 HDmWVEmZg7GcSbT0
62zQBUX0Xo3sDOquXyA2qzat4Gbq3FJeSTFEc3UQipHFBohb0qIkbWv2IeHC
m2nYjnaCi8P9o3y2nBn1rfzuHB2ctPnnTqK+eg=="

To verify:
```

with "foo.base64" containing the above signature:

```
$ openssl base64 -d -in foo.base64 -out sign.sha256

$ openssl dgst -sha256 -verify rsa.public -signature sign.sha256
domain.txt Verified OK
```

Authors' Addresses

Alex Brotman
Comcast, Inc

Email: alex_brotman@comcast.com

Stephen Farrell
Trinity College Dublin

Email: stephen.farrell@cs.tcd.ie