Abstract

This document specifies the use of the URI Resource Record Type to publish Decentralized Identifiers (DIDs) in the DNS.

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 February 26, 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

Decentralized Identifiers (DIDs) [W3C-DID] use a Uniform Resource Identifier (URI) scheme [RFC3986] to identify persons, organizations, or things in decentralized infrastructure, such as blockchains and distributed ledgers.

DIDs are structured around "methods", each method defining the syntax of the method specific identifier and the operations on the respective DIDs (See Section 3.2 of [W3C-DID] and [DID-METHODS]). For many methods, the method specific identifier is not human-friendly (for example, hash values referring to transactions on a blockchain). Most DIDs are therefore inherently hard to memorize for humans.

By referring to DIDs from the DNS, those hard to memorize identifiers can be discovered via well known, human friendly and widely established names. This document specifies how DIDs can be published in the DNS for discovery on the base of host names and email addresses.

Since DIDs use a URI scheme (‘did’), this specification leverages the existing URI DNS Resource Record Type (RRType) [RFC7553]. Records
are scoped using the `_did` global underscore node name, as described in Section 3.1.

2. Terminology

"Owner name", "Priority", "Weight" and "Target" refer to the respective fields of the URI RRType, as specified in Section 4 of RFC7553.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Use of the `URI` RRType

DIDs use an URI scheme (`did:`), so the most suitable option to publish DIDs in the DNS is the use of the `URI` RRType. During the development of this document, various alternatives were considered, see Section 6 for a list.

- When Decentralized Identifiers (DIDs) are published in the DNS, the `URI` RRType MUST be used.

3.1. Owner Name Scoping, Target

[RFC8552] describes the advantages of scoping an existing RRType over the definition (and complex deployment) of a new RRType. The "URI" RRType is specifically mentioned as one example where scoping is particularly useful (and part of the design).

When DIDs are published in the DNS

- the records MUST be scoped by setting the global (highest-level) underscore name of the URI RRset to `_did` (0x5F 0x64 0x69 0x64),
- and the Target field of all records in the RRset MUST contain a URI of the `did:` URI scheme.

3.2. Weight, Priority

The semantics of the Weight and Priority fields remain. When a client encounters a DID method it does not support, it SHOULD consider the respective DID "unreachable" for the purpose of record selection, and proceed to the URI with the next-lowest-numbered Priority, in accordance with Section 4.2 of RFC 7553.
4. Location of the Records

4.1. Host Names

In order to discover the set of DIDs associated with a Host Name, a client prepends the given Host Name with the '_did' global underscore name to create the Owner name, and then queries the resulting Query Name for the URI RRType set.

4.2. Email Addresses (Experimental)

To discover DIDs associated with email addresses, the (experimental) model from DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP [RFC7929] is used. A client prepares the email address following the procedure outlined in Section 5 in RFC7929, except that the second left-most label in step 5 of that procedure MUST be replaced with the label sequence '_mailto._did' instead to form the Query Name. Subsequently, the client performs a DNS query for the URI RRType (rather than the OPENPGPKEY RRType described in said section).

5. Example

The following example is a URI Resource Record which refers from the host name "example.net" to a Decentralized Identifier using the 'sov' method:

```
_did.example.net.  IN URI 100 10 "did:sov:1234abcd"
```

6. Considered Alternatives

During the development of this document, the following alternatives were considered: A dedicated RRType, TXT records, an Enumservice, Well-Known URIs, direct registration in the Service Name Registry. Updating the URI specification was found to be the option with the highest likeliness of interoperability combined with the lowest effort in standardization and implementation/deployment.

Furthermore, the Identifiers and Discovery Working Group of the Decentralized Identity Foundation (DIF) is considering a .well-known URL based approach to discovering DIDs from web sites.

7. Acknowledgements

Acknowledgements will be added here.
8. IANA Considerations

Per [RFC8552] IANA is requested to add the following entry to the DNS Underscore Global Scoped Entry Registry:

<table>
<thead>
<tr>
<th>RR Type</th>
<th>_NODE NAME</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>URI</td>
<td>_did</td>
<td>{THISRFC}</td>
</tr>
</tbody>
</table>

Table 1: Underscore Global Registry Entry Registration for '_did'

Note to RFC Editor: Please replace the above "{THISRFC}" text with a reference to this document’s RFC number.

Note that IANA has already created a provisional URI scheme registration for the ‘did:’ scheme itself.

9. Security Considerations

Most of the considerations outlined in the base specification of the URI RRType ([RFC7553]) also apply to the DID use case - particularly the concerns around downgrade attacks when the record is not signed with the help of DNSSEC. Note that the DID resolving process itself (out of scope of this document) can provide additional security information (such as a backreference to the DNS domain name).

Including a DID in the DNS allows to correlate that DID with DNS information, and is therefore NOT RECOMMENDED for DIDs which are supposed to be private.

10. Changes

[Note to RFC Editors: This whole section is to be removed before publication]

10.1. draft-mayrhofer-did-dns-02

- Updated attrleaf reference to RFC8552
- Changed author information for D. Klesev
- Added sentence on .well-known discovery scheme
10.2.  draft-mayrhofer-did-dns-01

- Email addresses further scoped with `_mailto._did`
- Changed protocol registration to attrleaf drafts
- Made clear requirements regarding use of the URI scheme
- Added privacy aspect to security considerations

10.3.  draft-mayrhofer-did-dns-00

- Initial version

11.  References

11.1.  Normative References


11.2.  Informative References


Authors’ Addresses

Alexander Mayrhofer
nic.at GmbH
Karlsplatz 1/2/9
Vienna 1010
Austria

Email: alex.mayrhofer.ietf@gmail.com

Dimitrij Klesev

Email: dimitrij.klesev@gmail.com