Network Working Group                                A. Mayrhofer
Internet-Draft                                         nic.at GmbH
Intended status: Standards Track                        D. Klesev
Expires: December 11, 2021

                                                    M. Sabadello
                                                 Danube Tech GmbH
                                                    June 9, 2021

### The Decentralized Identifier (DID) in the DNS
### draft-mayrhofer-did-dns-05

Abstract

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

Status of This Memo

Copyright Notice

Table of Contents

## 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 (such as hash values, referring to transactions on a
blockchain).  Most DIDs are therefore inherently hard to memorize for
humans.

By referring to DIDs from the Domain Name System (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 RFC
7553.

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.

o  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

o  the records MUST be scoped by setting the global (highest-level)
   underscore name of the URI RRset to '_did' (0x5F 0x64 0x69 0x64),

o  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 URI "unreachable" for the purpose of record

selection, and proceed to the record 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 the form the
Query Name, but in step 5 MUST use the string '_mailto._did' instead
of '_openpgpkey' as the second left-most label.  Subsequently, the
client performs a DNS query, but MUST use the URI RRType as Query
Type (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.
Using the URI RRType was found to be the option with the least impact
on existing specifications and highest interoperability potential.
Support for URI RRTypes is widespread in DNS software, which means
that implementation and deployment of the proposed protocol should be
possible without any changes to underlying infrastructure.

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. Implementations

DNS-DID is considered for implementation in the following frameworks
/ applications:

The "Registration" function of the "Fission" framework
(https://whitepaper.fission.codes/accounts/verifiable-claims)

## 8. Acknowledgements

Acknowledgements will be added here.

## 9. IANA Considerations

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

```
            +---------+-------------+-----------+
            | RR Type | _NODE NAME  | REFERENCE |
            +---------+-------------+-----------+
            | URI     | _did        | {THISRFC} |
            +---------+-------------+-----------+
```

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.

## 10. 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.  The "Linked Domain Service Endpoint" of a DID document
can be used to back-reference to the Domain which was originally used
to discover that DID.  Such a "closed loop" (similar to verifying DNS
reverse lookups against their corresponding forward lookups) would
increase the confidence in non-DNSSEC scenarios.

Including a DID in the DNS allows for correlation of that DID with
DNS information (and potentially registration information of that DNS
name).  Therefore DIDs which are supposed to be private SHOULD NOT be
added to the DNS.

## 11.  Changes

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

### 11.1.  draft-mayrhofer-did-dns-05

o  Adding "implementation" section

### 11.2.  draft-mayrhofer-did-dns-04

o  Reworded "Alternatives"

o  Added text about backreference using DID's Linked Domain Service
   Endpoint.

### 11.3.  draft-mayrhofer-did-dns-03

o  Updated DID spec to v1.0 document

o  Minor editorial changes to make text more clear.

### 11.4.  draft-mayrhofer-did-dns-02

o  Updated attrleaf reference to RFC8552

o  Changed author information for D.  Klesev

o  Added sentence on .well-known discovery scheme

### 11.5.  draft-mayrhofer-did-dns-01

o  email addresses further scoped with '_mailto._did'

o  Changed protocol registration to attrleaf drafts

o  Made clear requirements regarding use of the URI scheme

o  Added privacy aspect to security considerations

### 11.6.  draft-mayrhofer-did-dns-00

o  Initial version

## 12.  References

### 12.1.  Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119,
            DOI 10.17487/RFC2119, March 1997,
            <https://www.rfc-editor.org/info/rfc2119>.

[RFC7553]   Faltstrom, P. and O. Kolkman, "The Uniform Resource
            Identifier (URI) DNS Resource Record", RFC 7553,
            DOI 10.17487/RFC7553, June 2015,
            <https://www.rfc-editor.org/info/rfc7553>.

[RFC8174]   Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
            2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
            May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8552]   Crocker, D., "Scoped Interpretation of DNS Resource
            Records through "Underscored" Naming of Attribute Leaves",
            BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019,
            <https://www.rfc-editor.org/info/rfc8552>.

[W3C-DID]   W3C, W3C., "Decentralized Identifiers (DIDs) v1.0",
            February 2020, <https://www.w3.org/TR/did-core/>.

### 12.2.  Informative References

[DID-METHODS]
            W3C, W3C., "DID Method Registry", June 2018,
            <https://w3c-ccg.github.io/did-method-registry/>.

[RFC3986]   Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform
            Resource Identifier (URI): Generic Syntax", STD 66,
            RFC 3986, DOI 10.17487/RFC3986, January 2005,
            <https://www.rfc-editor.org/info/rfc3986>.

[RFC6116]   Bradner, S., Conroy, L., and K. Fujiwara, "The E.164 to
            Uniform Resource Identifiers (URI) Dynamic Delegation
            Discovery System (DDDS) Application (ENUM)", RFC 6116,
            DOI 10.17487/RFC6116, March 2011,
            <https://www.rfc-editor.org/info/rfc6116>.

[RFC6117]   Hoeneisen, B., Mayrhofer, A., and J. Livingood, "IANA
            Registration of Enumservices: Guide, Template, and IANA
            Considerations", RFC 6117, DOI 10.17487/RFC6117, March
            2011, <https://www.rfc-editor.org/info/rfc6117>.

   [RFC6335]  Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S.
              Cheshire, "Internet Assigned Numbers Authority (IANA)
              Procedures for the Management of the Service Name and
              Transport Protocol Port Number Registry", BCP 165,
              RFC 6335, DOI 10.17487/RFC6335, August 2011,
              <https://www.rfc-editor.org/info/rfc6335>.

   [RFC7929]  Wouters, P., "DNS-Based Authentication of Named Entities
              (DANE) Bindings for OpenPGP", RFC 7929,
              DOI 10.17487/RFC7929, August 2016,
              <https://www.rfc-editor.org/info/rfc7929>.

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


   Markus Sabadello
   Danube Tech GmbH
   Annagasse 8/1/8
   Vienna  1010
   Austria

   Email: markus@danubetech.com