Network Working Group
Internet-Draft
Updates: 7553 (if approved)
Intended status: Standards Track
Expires: February 7, 2019

A. Mayrhofer
D. Klesev
nic.at GmbH
M. Sabadello
Danube Tech GmbH

August 6, 2018

The Decentralized Identifier (DID) in the DNS
draft-mayrhofer-did-dns-00

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 7, 2019.

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 most methods, the method specific identifier content 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 such a protocol, and describes how DIDs can be discovered on the basis of host names and email addresses.

Since DIDs use a URI scheme ('did'), this specification leverages the existing URI DNS Resource Record Type [RFC7553] for that purpose. However, the original specification of the URI RRType limits the possible values for the service parameters of the Owner name, effectively disallowing the DID use case described above.

In order to allow inclusion of DIDs in the DNS, this document updates RFC7553 to allow the string '_did' as a service parameter in the Owner name of the URI RRType. For a detailed discussion, see Section 3.

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. The '_did' Service Parameter for the URI RRType

As described in Section 1, RFC 7553 limits the set of strings allowed as service parameters in the Owner name of the URI RRType. Valid strings have to be registered in either the "Service Name and Transport Protocol Port Number Registry" [RFC6335] or the "Enumservice Registrations" registry [RFC6117]. However, both registries are unsuitable for DIDs because:

- DIDs are not tied to a specific transport protocol, hence a registration in the Service Name registry is not possible (See Section 8.1.1. of RFC6335).

- Enumservice registrations apply to E.164 Number Mapping (ENUM) [RFC6116] only, while the use case for DIDs in the DNS extends beyond that limited scope.

3.1. Owner Name

Given the considerations above, it is believed that the most effective way to allow for DIDs in the URI RRType is extending the set of allowed service parameters used in the Owner name as follows:

- In addition to the choices listed in Section 4.1 of RFC7553, the service parameter of the Owner name in the URI RRType MAY be set to '_did' (without quotes).

- When '_did' is used as service parameter in a URI DNS record, the Target field 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. See 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' Service Parameter to create the Owner name, and then queries for the URI RRType set (RRSet) of the resulting Query Name.

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 set to '_did' instead. 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 impact on standardization and implementation.

7. Acknowledgements

Acknowledgements will be added here.

8. IANA Considerations

In order to prevent unintended name space collisions, IANA is requested to reserve the string 'did' (0x64 0x69 0x64) in the Service Name and Transport Protocol Port Number Registry. The reason that a reservation (rather than an assignment) is requested is because according to Section 8.1.1. of RFC6335, a transport protocol is REQUIRED with such a registration. However, DIDs are not related to a specific transport protocol, and so a reservation (if possible) seems to be the only way.

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).

10. Changes

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

10.1. draft-mayrhofer-did-dns-00

Initial version

11. References

11.1. 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>.

[W3C-DID] W3C, W3C., "Decentralized Identifiers (DIDs) v0.11", July 2018, <https://w3c-ccg.github.io/did-spec/>.

11.2. 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
nic.at GmbH
Karlsplatz 1/2/9
Vienna 1010
Austria

Email: dimitrij.klesev@nic.at

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

Email: markus@danubetech.com