

The Decentralized Identifier (DID) in the DNS

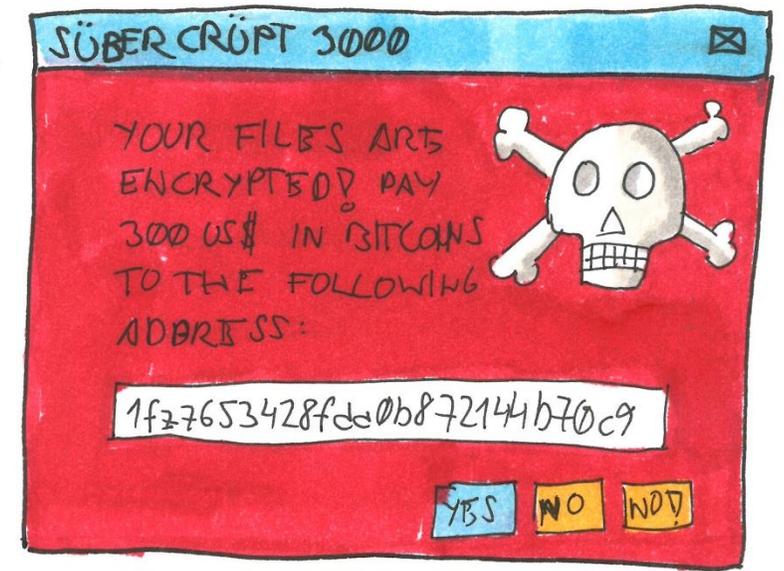
draft-mayrhofer-did-dns-00

A. Mayrhofer (nic.at) - D. Klesev (nic.at) - M. Sabadello (danubetech)

alexander.mayrhofer@nic.at

Background – Blockchain Addressing

- „Distributed Ledgers“ (read: Blockchains) typically use Adresses to identify resources
 - 3E53XjqK4Cxt71BGeT2VhpcotV8LZ853C8
- Adresses lack identification of the Blockchain / Ledger on which they can be found
 - (above example is a bitcoin* address)
- Not suitable for identification
 - (at least on a global scale)
 - Ambiguity



Bite Reflexes.

- „Let’s put it into the DNS“
 - Makes it human friendly
 - Globally available resolution
- But, how exactly?
- Decisions, decisions..
 - TXT ?
 - RRTYPE ?
 - CLASS ?
 - Owner Name Structure?

Tylopoda Considerations.



Exhibit B:
Our „let's put it into the
DNS“ draft

Exhibit C:
You. And me!

Exhibit A:
The Poor (smiling??)
Camel

Background II – Decentralized Identifiers*

- Work of the W3C Credentials Community Group (soon to be „upgraded“ to a Working Group)
- URI-Scheme „did“ (Provisional Registration)
- Hierarchical Scheme:

`did:btrc:xzuc-wzcq-qqpq-qupuzs8`
URI-Scheme:Method:Method-specific Identifier

- Bingo! RFC 7553: DNS URI RRtype!

*<https://w3c-ccg.github.io/did-spec/>

draft-mayrhofer-dns-did-00

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

- **RRType + Owner Name:** RFC 7553 – URI RRType
- **Email to DID:** RFC 7929 – DANE for OpenPGP
- **Service Parameter:** Existing IANA-Registry*
 - But requires Port or at least Protocol
 - Or an ENUMservice
 - (Current) Solution: Update RFC7553 to allow „_did“ as well besides the two types above..

*<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

Running Code

- uniresolver.io

The screenshot displays the DIF Universal Resolver interface. At the top, the logo and title 'DIF Universal Resolver' are visible. Below this, there is an input field labeled 'did' containing the text 'ssi.labs.nic.at'. To the right of the input field are two buttons: a blue 'Resolve' button and a black 'Clear' button. Below the input field, there are four tabs: 'RESULT' (which is selected), 'DID DOCUMENT', 'RESOLVER METADATA', and 'METHOD METADATA'. Under the 'RESULT' tab, the section is titled 'Parser'. Below this title is a table with the following structure:

DID	Method	ID	Service	Path
did:sov:stn:r1dwAJxcoG7EPiioGMz7h	sov	stn:r1dwAJxcoG7EPiioGMz7h		

Below the table, there is a section titled 'Public Key' with the following text:

```
Ed25519VerificationKey2018
~MEC1mTDJEp7q9b8nQeStZp
```

Next steps.

- Update of RFC7553 the most efficient way?
- Easiest: Entry for a protocol-independent „Service Parameter“
 - Is that possible?
 - Question to IANA pending [#1118333]
- Way forward with the draft?