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 Adressing

• „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

*slightly modified
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?
Tylopodae Considerations.

Exhibit A: The Poor (smiling??) Camel

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

Exhibit C: You. And me!

Photo: Felice Beato on the Nile Expedition to relieve Khartoum, ca. 1884
Background II – Decentralized Identifiers*

• Work of the W3C Credentials Community Group (soon to be „upgraded“ to a Working Group)
• URI-Scheme „did“ (Provisional Registration)
• Hierachical 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/
• **RRType + Owner Name:** RFC 7553 – URI RRTyp
• **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
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?