Bridging Perspectives: Understanding the Challenges and Opportunities in Current DNS Integrations

Swapneel Sheth
Verisign
ICANN DNS Symposium 2023
September 5, 2023
Agenda

- Global DNS diversification via integrations
- DNS-based integrations
- Server-based integrations
- Challenges of managing namespace integrations
- Responsible integration
Diversification of Global DNS

Register in Global DNS → Relate to Application

- Email
- Web

New Applications?
### Partial List of Groups Discussing DNS Integrations

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>W3C DID</td>
<td>did:dns/did:web</td>
</tr>
<tr>
<td>Bluesky AT Protocol</td>
<td></td>
</tr>
<tr>
<td>Microsoft Entra</td>
<td></td>
</tr>
<tr>
<td>Ethereum Name Service</td>
<td></td>
</tr>
<tr>
<td>Tezos Domains</td>
<td></td>
</tr>
<tr>
<td>IETF keytrans BoF</td>
<td></td>
</tr>
<tr>
<td>IETF DBOUND2 BoF</td>
<td></td>
</tr>
<tr>
<td>ICANN Participants</td>
<td></td>
</tr>
<tr>
<td>IETF DNSOP</td>
<td></td>
</tr>
<tr>
<td>IETF ACME</td>
<td></td>
</tr>
<tr>
<td>IRTF DIN</td>
<td></td>
</tr>
<tr>
<td>CAB Forum</td>
<td></td>
</tr>
</tbody>
</table>
## Types of DNS Integrations

<table>
<thead>
<tr>
<th>DNS-based</th>
<th>Server-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data needed to facilitate the integration primarily exists in DNS records</td>
<td>• Data needed to facilitate the integration primarily exists on a server, blockchain, or other external source</td>
</tr>
</tbody>
</table>
DNS-based Integrations

Associates a DNS domain name with another resource using DNS records

Classic example is A record for web hosts

New example is TXT to link to a W3C decentralized identifier as proposed by Bluesky
DNS-based: Bluesky Social Handle

- **Bluesky uses DNS domain names** as usernames, e.g., example.bsky.app

- Registrant can utilize their own DNS domain name in Bluesky by:
  1. Use Bluesky App to generate the data needed for the required TXT record
  2. Configure the “_atproto” TXT record in the domain’s zone with data from step 1
  3. Verify the TXT in Bluesky App to finalize

**Example: Bluesky Handles**

Enter the domain you want to use
@ eg alice.com

Add the following record to your domain:
Domain: _atproto.
Type: TXT
Value: did=did:plc:ewvi7nxzyoun6zhxrh5s64oiz

Source: Bluesky Blog
DNS-based: IPFS DNSLink TXT Records

- A **method** that uses a DNS domain name to refer to an IPFS content hash via a TXT record

- Registrant can utilize their DNS domain name in IPFS ecosystem via DNSLink by:

  1. Configure a TXT record in the domain’s zone per the DNSLink specification:

     ```text
     _dnslink.example.com. IN TXT "dnslink=/ipfs/bafyb...hcjze"
     ```

  2. Interact with applications that have support for DNSLink to resolve IPFS content via the DNS domain name
DNS-based Integrations to Prove Control

Can also be used to prove control of a domain but the rest of the integration is managed outside DNS.

Classic example is a web certificate granted by proof of DNS data.

New examples are blockchain namespaces like Ethereum Name Service and Tezos Domains using DNSSEC + TXT records.
DNS Control-based: On-Chain ENS DNSSEC

- DNSSEC-based approach (introduced by ENS in 2018)
- Registrant can utilize their DNS domain name in ENS by:
  1. Enable DNSSEC
  2. Configure the “_ens” TXT record in the domain’s zone
  3. Compile a DNSSEC chain of trust
  4. Submit a blockchain transaction with the DNSSEC chain of trust for verification by the ENS DNSSEC smart contract

Example: Chain of Trust for ENS DNSSEC

Source: ENS Blog Post
DNS Control-based: Discord

• Discord will be **adding support** for verifying control of a DNS domain name to link to a user’s Discord account

• Registrant can utilize by:
  1. Configure TXT record “_discord”:
     
     `_discord.example.com. 3600 IN TXT "<challenge>"`

  2. Users will see a verified domain name as part of the registrant’s Discord account

Source: Discord Previews
Server-based Integrations

Associates a DNS domain name with another resource based on content hosted on a web server.

Classic example is ACME protocol's server-based approach to receive a certificate.

New example is W3C decentralized identifier did:web.
Server-based: Microsoft Entra

- Entra utilizes DNS domain names to provide trust and familiarity to users who interact with the Entra platform.

- Registrant can **verify their domain** by:
  1. Create a DID (e.g. did:web)
  2. In the Entra portal, download did-config file
  3. Store did-config file on domain’s web server
  4. Verify in Entra portal that did-config is correctly configured and accessible

Source: Entra documentation
Server-based: Fediverse Alias Usernames

- Mastodon uses an email style of username
  - @example@mastodon.social is a user by the name “example” hosted on the Mastodon server “mastodon.social”

- Users can alias from a domain to their Mastodon account:
  - Configure a well-known endpoint on the registrant’s server that serves a specific JSON blob associated with Fediverse data:
    - https://example.com/.well-known/webfinger
  - @example@example.com → @example@mastodon.social
Potential Concerns with Current Approaches

- Domain name lifecycle management
- Interoperability
- Support for new use cases
- DNS namespaces may have different policy emphases
- Commitment to a particular integration is unclear
Considerations with Existing DNS Integrations

- Control
- Domain Lifecycle
- Alignment
- Utility
Standardizing Responsible DNS Integrations?

Domain Name System (DNS)

New Applications

DID斯

Blockchains

Identity

Responsible DNS integration