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

Swapneel Sheth

Verisign

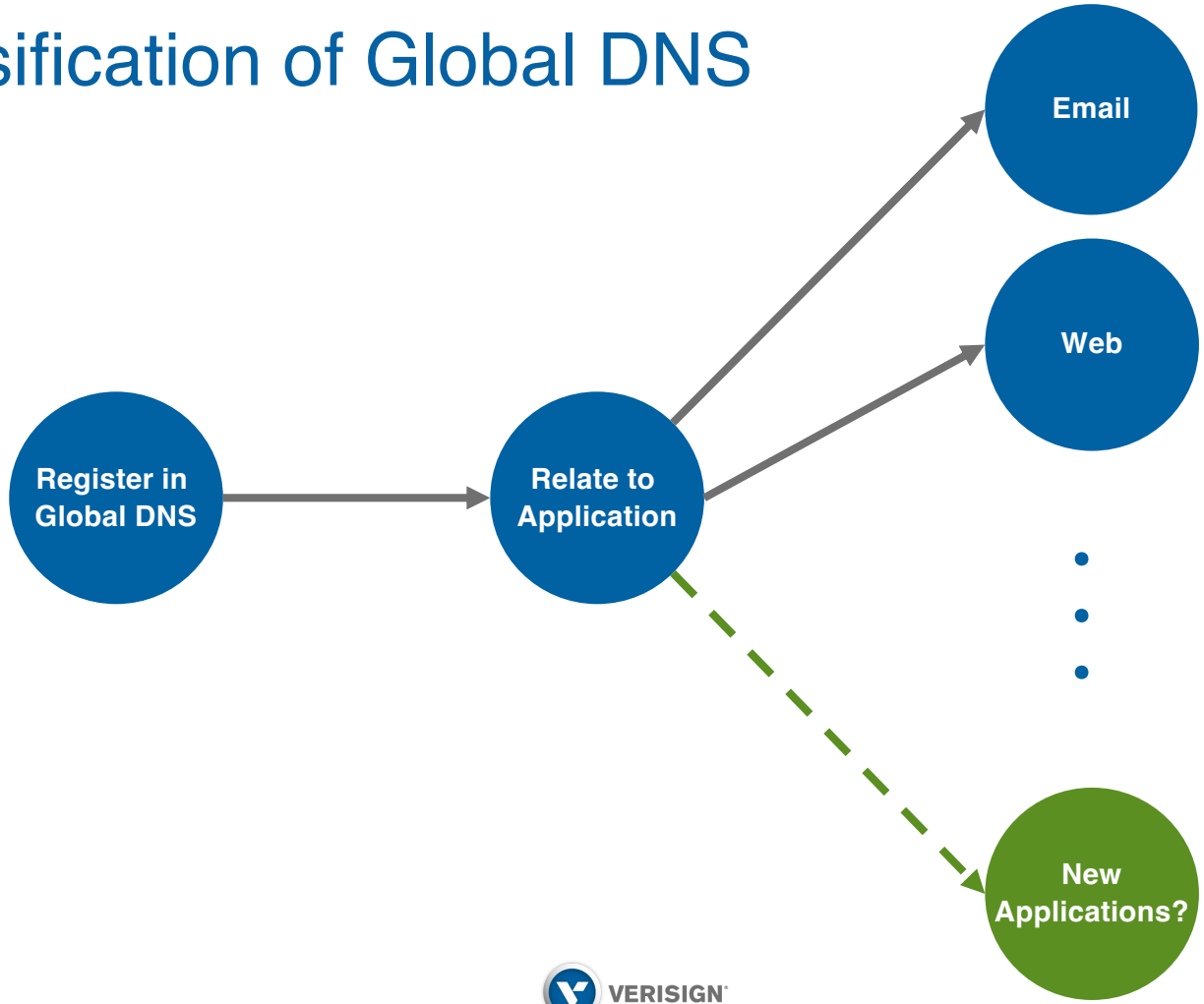
ICANN DNS Symposium 2023

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



Partial List of Groups Discussing DNS Integrations

W3C DID did:dns/did:web	Bluesky AT Protocol	Microsoft Entra	Ethereum Name Service
Tezos Domains	IETF keytrans BoF	IETF DBOUND2 BoF	ICANN Participants
IETF DNSOP	IETF ACME	IRTF DIN	CAB Forum

Types of DNS Integrations

DNS-based

- Data needed to facilitate the integration primarily exists in DNS records

Server-based

- Data needed to facilitate the integration primarily exists on a server, blockchain, or other external source

DNS-based Integrations

Associates a DNS domain name with another resource using DNS records

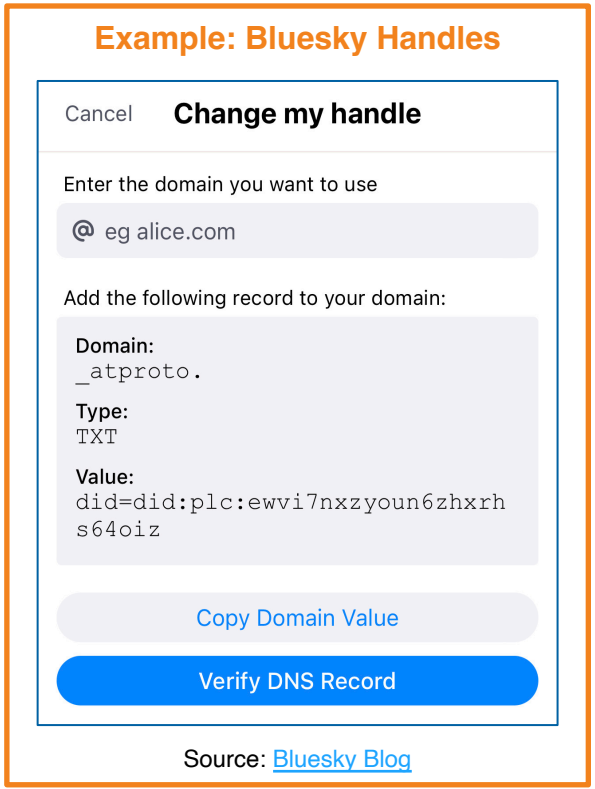
Classic example is A record for web hosts

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



DNS-based: IPFS DNSLink TXT Records

- A method that uses a DNS domain name to refer to an IFPS 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:

     ```
     _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

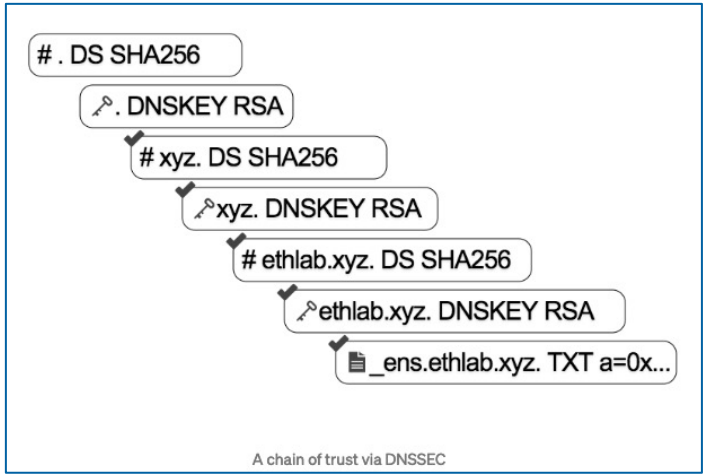
Classic example is a web certificate granted by proof of DNS data

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

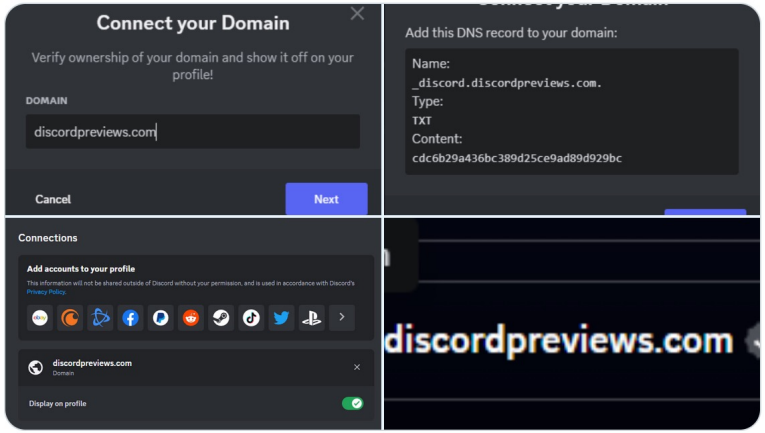
- Discord will be adding support for verifying control of a DNS domain name to link to a user's Discord account

- 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

Example: Discord Previews



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

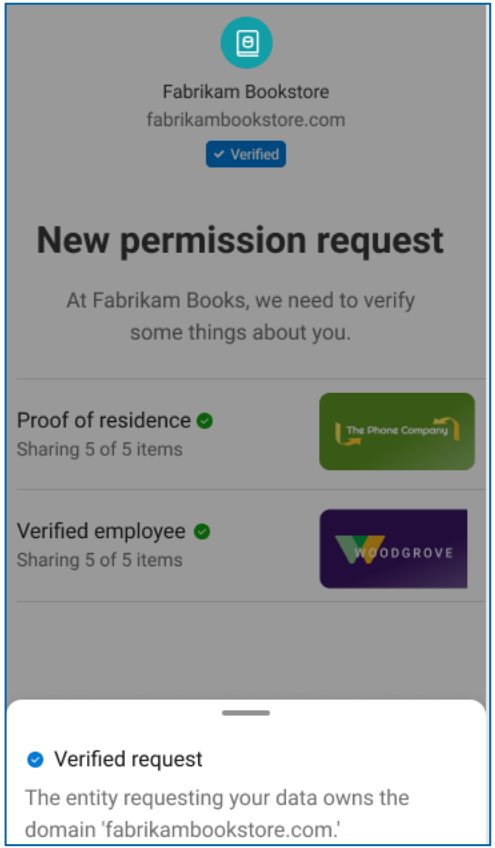
New example is W3C decentralized identifier did:web

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

Example: Microsoft Entra



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

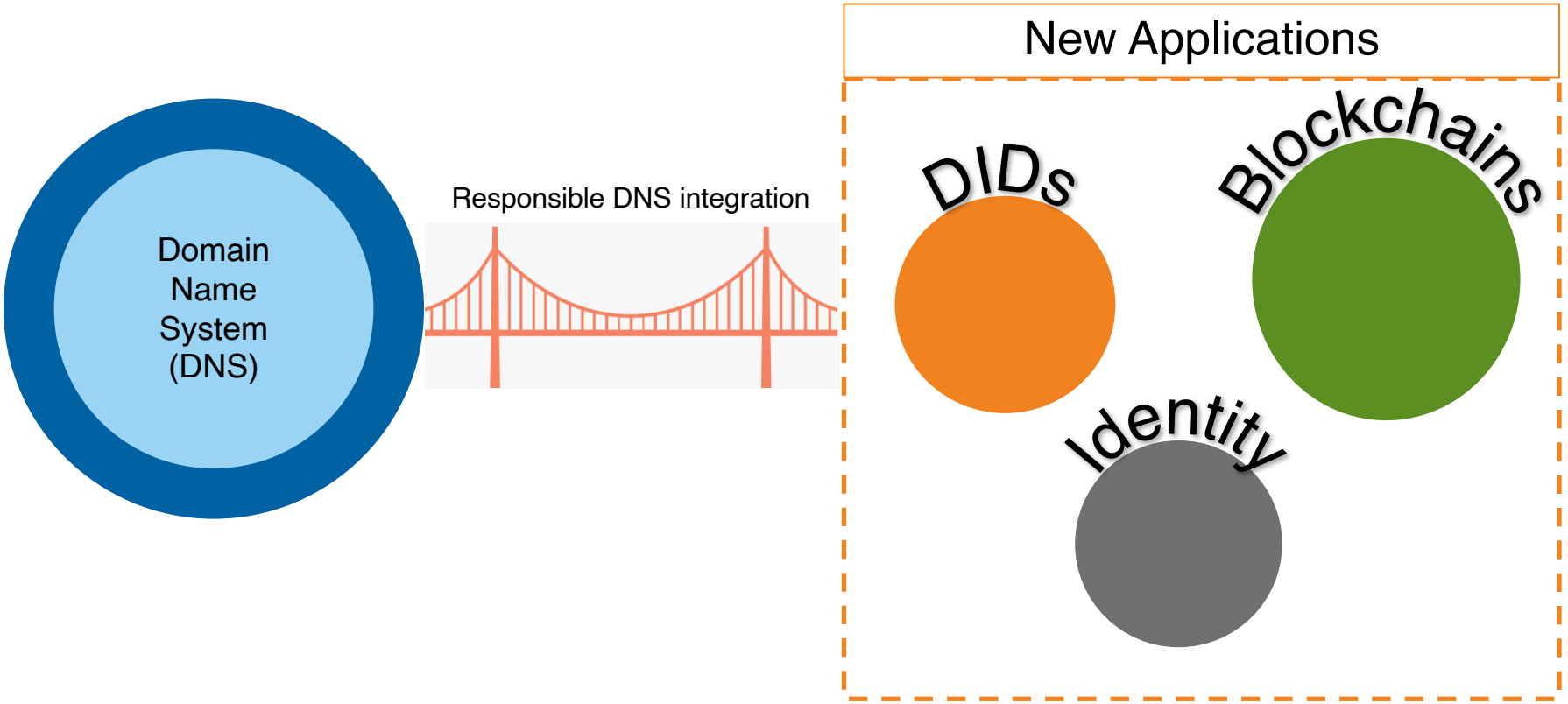
Control

Domain Lifecycle

Alignment

Utility

Standardizing Responsible DNS Integrations?



VERISIGN®