Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 10 April 2026

S. Sheth
A. Kaizer
Verisign Labs
B. Newbold
Bluesky, PBC
N. Johnson
ENS Labs

7 October 2025

Integration of DNS Domain Names into Application Environments: Motivations and Considerations
draft-ietf-dnsop-integration-01

Abstract

This document describes considerations when integrating a DNS domain name into an application environment. Goals of this document include minimizing conflicts between the global DNS and applications that integrate with the global DNS, providing a consistent user experience (unique identifier across environments), and extending the security, stability, and resiliency of the global DNS. While all sources of potential concern cannot be enumerated in one document, accounting for at least the considerations discussed here should improve the security posture of both the global DNS and integrating applications.

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 10 April 2026.

Copyright Notice

Table of Contents

1. Introduction

This document describes considerations when integrating a DNS domain name into an application environment. While the considerations may apply to other systems that use a domain-name based syntax, this document is targeted at domain names from the "global DNS" as defined in [RFC2826] and [RFC9499], i.e., the DNS namespace as managed and governed by ICANN's multistakeholder model. The rest of this document proceeds under this framing.

Domain names from the global DNS have long been used as identifiers in applications. In the early days, domain names were associated with TELNET hosts, File Transfer Protocol (FTP) servers, and email services. Later, domain names were adopted for web browsing. More recently, blockchain applications, decentralized protocols, and

social media platforms have emerged as new use cases for domain names. How a domain name is enabled for use as an identifier in each of these applications is known as a DNS integration.

Given the ever-increasing number of application environments using or proposing their own DNS integrations, there is a need to raise awareness about considerations that such applications should account for in order to provide a "responsible" DNS integration. A responsible DNS integration can be defined as one that allows a domain name to be used within an application environment in a way that provides a consistent user experience (unique identifier across environments) and extends the security, stability, and resiliency of the global DNS.

In support of the development of responsible DNS integrations, this document describes some considerations that DNS integrations should account for. Failure to account for such considerations may result in inconsistent user experience across environments and risks to the security, stability, and resiliency of the global DNS from an application perspective. While all sources of potential concern cannot be enumerated in one document, accounting for at least the considerations discussed here should improve the security posture of both the global DNS and integrating applications.

1.1. Intended Audience

This document is targeted at developers of applications that provide or are considering an integration with the global DNS, e.g., to use domain names as an identifier in their application. Applications might be motivated to integrate with the global DNS for various reasons: global consistency, universal acceptance, human-readable identifiers, stability, flexibility, verifiability, and to utilize the reputation registrants may have already developed around their use of a domain name.

This document does not prescribe specific mechanisms about how to perform a DNS integration, but rather provides considerations that apply broadly to DNS integrations.

Applications may find value in using this document as a checklist that, if ensuring each consideration is accounted for, can decrease outcomes that could negatively impact the security, stability, and resiliency of the application and the global DNS.

2. Terminology

This document uses the terminology from [RFC9499] as a baseline. Additional terms applicable to DNS integrations are provided here in alphabetical order:

* Application environment: An application, platform, or protocol
* DNS integration: How a domain name is enabled for use as an identifier in an application environment
* Responsible DNS integration: Takes into account qualities and considerations that provide a consistent user experience and extends the security, stability, and resiliency of the global DNS
* Synchronization: The property that a domain name integrated into an application environment aligns with its state in the global DNS

3. Considerations for a DNS Integration

This section provides considerations that a DNS integration should account for in their specification design. Failure to account for such considerations may result in user confusion, name collisions between an application and the global DNS, or other security related concerns. The exact risks depend on the context and design of the integration and are out of scope for this document.

3.1. Domain Name Lifecycle

A DNS integration should account for domain name lifecycle events. Some examples of lifecycle events include expiration, change in DNSSEC status, or technical changes that affect the integration such as the removal of an expected resource record. Such lifecycle events might result in a change of control or status of the domain name compared to when it was originally integrated that could require one of the parties involved in the DNS integration to take some action to stay synchronized with the state of the domain name in the global DNS.

Failure to account for the domain name lifecycle might result in a DNS integration allowing users other than the current registrant of the domain name to control the domain name in the integration which could lead to confusion.

3.2. Domain Control Validation

A DNS integration should implement validation checks to ensure only the DNS registrant or an authorized party associated with the domain name can establish the integration. Some examples of domain control validation include storing data in DNS [I-D.ietf-dnsop-domain-verification-techniques] or storing evidence on a server referenced by a domain name, e.g., at a well-known endpoint as described in [RFC8615].

Failure to perform validation might result in a DNS integration allowing users other than the current registrant of the domain name to control the domain name in the integration which could be confusing. This could lead to a security risk which may break end user trust.

3.3. Completeness

A DNS integration should allow any domain name that meets the integration’s technical criteria to be integrated. Not doing so excludes domain names from participation for non-technical reasons, which could lead to registrant confusion if they are not able to associate their domain name.

DNS integrations should also be aware that global DNS domain names are not limited to ASCII characters, e.g., as described in [RFC5890]. Failure to account for such domain names may lead to inadvertent exclusion which could also lead to registrant confusion.

3.4. Synchronization

A DNS integration should provide mechanisms to handle cases where an integrated domain name is no longer synchronized. How often to execute such mechanisms will vary by DNS integration and the use cases supported. For example, a DNS integration that supports financial use cases may check more often than a DNS integration that shows a verification of domain control badge on a social media profile.

In general, the entity providing the DNS integration is primarily responsible for ensuring synchronization with the global DNS. A DNS integration can allow other users to invoke one or more mechanisms, but this should not be solely relied upon as there are no guarantees that users will do so. For example, if a domain name expires the registrant that originally interacted with the DNS integration may not be interested, aware, or available to invoke the mechanisms to remove the domain name.

A designer of a DNS integration should also be cognizant that executing these mechanisms too frequently may result in rate limiting. This may also occur if multiple integrated domain names share the same infrastructure which increases the potential that rate limits would be triggered. Consequently, a DNS integration should account for this potential in their mechanisms.

3.5. DNS Protocol Evolution

A designer of a DNS integration should be aware that the DNS protocol will evolve over time and such evolutions might impact their DNS integration. For example, DNSSEC algorithms have changed over time as new algorithms are added, and existing algorithms are deprecated. Failure to account for such changes might pose a security risk, lead to user confusion, or cause a lack of interoperability with the current state of the global DNS.

3.6. Identifier Attribution

A designer of a DNS integration should not assume a domain name is a persistent identifier that always associates to the same registrant. Domain names may be deleted and re-registered or be transferred, which might result in the previous registrant no longer being associated with the domain name. DNS integrations should account for such changes in control to avoid potential confusion, e.g., content being mis-attributed to the current registrant that belonged to a previous registrant.

Additionally, domain names may be exposed to temporary interruptions such as system downtime, DNS hijacking, or web server compromise. Such events may unexpectedly change who can utilize the domain name or impact the ability of a DNS integration from checking the status of the domain name. DNS integrations should have mechanisms in place to handle and recover from such issues, including allowing a registrant to re-integrate the domain name.

3.7. Variety of DNS Management User Interfaces

A DNS integration might request a user follow certain actions to enable the integration. For example, a TXT record might need to be set or DNSSEC might need to be configured. However, each DNS management user interface might expose how to achieve the required actions in different ways. This introduces friction to the integration process as the user might only know what they need to do -- e.g., add a TXT record -- but not necessarily how to do it. Integrations might provide advice for how to perform such actions for some interfaces, but it is not feasible to do so for all.

3.8. DNS Record Type Support

A DNS integration might utilize record types that are not widely supported at DNS providers. For example, new DNS record types will take time to be rolled out to DNS providers or a DNS provider might opt not to support a particular record type. To avoid such challenges, a DNS integration should provide alternatives, such as a different record type that is expected to be more broadly deployed to ensure users can participate.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

This document does not introduce new protocol artifacts with security considerations, however, DNS integrations should account for general DNS related issues including confusable characters such as those discussed in Section 4.4 of [RFC5890] and resource capacity considerations.

Resource capacity in a DNS integration impacts who is capable of performing the necessary steps to participate in or validate the integration. For example, if an integration requires DNSSEC then some clients might not be able to perform the necessary cryptographic operations on their own such as IoT devices or human users performing manual validation. DNS integrations should be cognizant of this potential gap in capabilities and how it could impact their DNS integration.

Minimizing conflicts between the global DNS and applications that integrate with the global DNS is one of the goals of this document. While all sources of potential conflict cannot be enumerated, this effort should improve the security posture of both the global DNS and integrating applications through highlighting considerations to account for when providing a DNS integration.

6. Informative References

[I-D.ietf-dnsop-domain-verification-techniques]
Sahib, S. K., Huque, S., Wouters, P., and E. Nygren, "Domain Control Validation using DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-domain-verification-techniques-04, 3 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-domain-verification-techniques-04>.

[RFC2826] IAB, "IAB Technical Comment on the Unique DNS Root", RFC 2826, DOI 10.17487/RFC2826, May 2000, <https://www.rfc-editor.org/info/rfc2826>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

Appendix A. Integration Lessons Learned

A.1. Bluesky and AT Protocol

Bluesky is a social media application built on the atproto (AT Protocol) network. In atproto, account identities are rooted in the Decentralized Identifier (DID) system, a W3C standard. Most DIDs are not human readable, so every account is also associated with a domain name, referred to as a "handle". Handles are for display only: they are not used in persistent references (URIs), and can change any time without breaking social graph connections. The handle/DID relationship must be verified bi-directionally, and DNS TXT records are one mechanism to verify the handle-to-DID direction. Bluesky handles are a DNS Integration.

DNS was chosen as the handle namespace partially for technical maturity, efficiency, and cost reasons. Registering a new handle needed to be fast (second-level latency), zero-cost, and reliable (near-zero downtime). DNS meets all of these requirements. The atproto network is design to accommodate billions of accounts, and DNS has also been shown to scale to hundreds of millions of registered domains without significant infrastructure burden. Service providers can use sub-domains as handles, and allocate them in large numbers even more efficiently.

Bluesky is a small young company building a novel network protocol. DNS is a mature and broadly adopted technology, meaning developers are already familiar with it and have software implementations and infrastructure at hand. The system is financially sustainable with a international multi-stakeholder governance structure, which means developers can build on it with confidence.

DNS is global, distributed, and consistent which are important for a distributed network. Independent service providers and software clients see the same view of the domain system, which means that end users will have a coherent experience regardless of provider or client.

Domain names are well established in society. Domain names are conceptually familiar and recognizable to most network users. Policies, legal precedent, and dispute resolution procedures are mature across many jurisdictions. These help address the perential challenges of impersonation and trademark disputes. In particular, many culturally relevant institutions and individuals already have domain names with an established reputation. The flexibility of DNS allows those existing domains to be reused in a new context.

To maximize these benefits, it is important that handle validation is consistent and reproducible by any party. Any valid domain name (hostname) can be used as a handle and that all handles are valid globally resolvable domain names. This ensures that every network service can resolve any handle in the network, without requiring special DNS software. Use of the TXT record type has broad support in both client software and in DNS management interfaces. Limited use of caching helps reduce breakage due to short network service downtimes, while still ensuring that handle validity lifetime is tied to domain registration lifetime. In other words, changes in domain control are reflected in changes on handle validity within a reasonable time window, reducing the chance of misattribution. The atproto handle specification text largely defers to IETF DNS standards, with the goal of maintaining compatibility as norms and best practices evolve over time.

A.2. Ethereum Name Service

ENS integrates DNS names to provide a unified namespace across blockchain and traditional applications. This expands ENS’s usefulness by incorporating the millions of existing DNS names into the system, allowing people to use familiar identifiers that are already associated with their organization.

The primary challenges have revolved around reliably identifying public suffixes, and identifying the authorized user for a domain. Early versions of the integration made unfounded assumptions, such as the ownership of nic.tld form domains. This draft will help future implementers avoid such pitfalls.

Appendix B. Change Log

00: Initial draft of the document as adopted by DNSOP

01: Incorporating initial feedback from call for adoption and early ARTART/SECDIR reviews

Acknowledgements

The authors would like to acknowledge the following individuals for their contributions to this document: TBD.

Authors' Addresses

S. Sheth
Verisign Labs
12061 Bluemont Way
Reston
Email: ssheth@verisign.com
URI: https://www.verisignlabs.com/

A. Kaizer
Verisign Labs
12061 Bluemont Way
Reston
Email: akaizer@verisign.com
URI: https://www.verisignlabs.com/

B. Newbold
Bluesky, PBC
Email: bryan@blueskyweb.xyz
URI: https://bsky.social/about

N. Johnson
ENS Labs
Email: nick@ens.domains