Internet Engineering Task Force
Internet-Draft
Intended status: Best Current Practice
Expires: 24 October 2025

S. Sheth
A. Kaizer
Verisign Labs

22 April 2025

Best Practices for Persistent References in DNS
draft-sheth-identifiers-dns-00

Abstract

This document details some best practices for Application Service Providers who allow associations between a global DNS domain name and use case specific references using DNSSEC to provide a globally consistent, cryptographically verifiable association. Such a mechanism is needed when nonce-based domain control validation is not practical, such as use cases where each participant wants to confirm the association independently. As such, no single Application Service Provider exists to provide and validate a nonce to prove domain control that would satisfy other participating Application Service Providers.

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 24 October 2025.

Table of Contents

1. Introduction

Some Application Service Providers support using a global DNS domain name in the applications they provide. To do so, these providers require a user to provide evidence of the user's intent to associate the user's domain name with the user's presence in an application, e.g., with a use case specific identifier. While nonce-based domain control validation (DCV) has long been used for this purpose, DCV may not be practical when the association is persistent and where multiple Application Service Providers want to confirm the association independently.

Where a nonce-based approach is not practical, Application Service Providers have been observed requiring users to store use case specific references that do not include nonces in one or more DNS records. This is used to establish an association between the domain name and the user's presence for that use case. The records set by the user are then persisted for as long as the user continues to opt into this association, much like how A or AAAA records are persisted for as long as a user is using the IP addresses to host their domain name.

This approach has found traction in several contexts, such as those described in Appendix A. One example is certificate issuance using the Certification Authority Authorization (CAA) record found in [RFC8659] and the proposed cryptographically-constrained domain validation found in [I-D.birgelee-lamps-caa-security]. For this use case, the domain name is associated with one or more certificate authorities who are authorized to issue certificates for that domain name. The CAA record can limit certificate mis-issuance risks but does require all certificate authorities have the ability to check the CAA record and observe the same record data to achieve this outcome.

Another example is the use of domain names as social media handles, e.g., as seen in the Authenticated Transfer (AT) Protocol that powers decentralized social media applications like Bluesky [atproto]. For this use case, the domain name is associated with an AT Protocol identifier via a TXT record or HTTPS well-known endpoint. Any Application Service Provider in the AT Protocol ecosystem, such as Bluesky, can then use the domain name as a user's handle by checking this association.

Support for these use cases is not without challenges. First, Application Service Providers need a globally consistent, spoofing resistant view of the association so they can agree on the state of the domain name. Second, Application Service Providers need to continually assess the association, e.g., to identify when a domain name has opted out of the association or no longer exists. Failure to do so may result in interoperability or security concerns.

This document provides some best practices to ensure that persistent references are appropriately maintained when using DNS-based methods. Other methods such as those based on HTTP are out of scope.

1.1. Contrast with Domain Control Validation

The primary difference between this document and the best practices for Domain Control Validation (DCV) in [I-D.ietf-dnsop-domain-verification-techniques] is the persistence and content of the information used to associate a domain name with the user's presence at an Application Service Provider. DCV uses time-bound random tokens, i.e., nonces, to indicate that a user controls a domain name at a point in time. This is in contrast to the persistent association stored in DNS that is described here which uses DNSSEC to authenticate the user's ongoing intent to associate the domain name with a particular use case.

There are scalability challenges when attempting to use DCV for persistent references. For example, if there are N independent Application Service Providers for a particular use case, then at least N independent nonces may be needed so that the user can prove to each provider that they control the domain name. Additionally, nonce-based challenges would need to be re-issued as often as each Application Service Provider wants to re-verify the association. If N or the rate of re-issuance is too high, the workload can quickly become impractical for a user to maintain. This contrasts with this document where the requirement to use DNSSEC supports a globally consistent view of the associations regardless of how large N is.

1.2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the terminology from [RFC9499] and [I-D.ietf-dnsop-domain-verification-techniques] as a baseline with minor modification as follows:

* Application Service Provider: an internet-based provider of a service, for e.g., a Certification Authority or a social media platform. These services often require a User to establish an association between the domain name and the user's presence for a use case supported by a provider. The Application Service Provider may be implementing a standard protocol for this association (such as [RFC8659]) or they may have their own specification that one or more other providers may also utilize.

* User: the registrant or operator of a domain in the DNS who needs to establish an association between the domain name and the user's presence for a use case supported by an Application Service Provider.

2. Requirements

These requirements provide best practices to Application Service Providers that develop methods to provide an association between a global DNS domain name and a use case that is stored as one or more persistent references in the DNS. The best practices are not exhaustive but instead focus on establishing a baseline of consistency as it relates to the DNS component of such a system. Each Application Service Provider may have additional criteria or considerations as it pertains to their own use cases and this document should not be taken as limiting such additional criteria.

2.1. Record Types and Labels

The record types and labels used SHOULD be precise enough that any registrant, DNS administrator, or similar can determine the intent of each record based on their content and DNS label. This helps users understand and appropriately manage their DNS zone and avoid service interruption by accidental removal of an association.

The record types utilized are at the discretion of the Application Service Providers.

It is RECOMMENDED that Application Service Providers use an underscore scoped "_<USE_CASE_RELEVANT_NAME>-persist" label to appropriately scope their use case if a use case specific resource record type is not used. This avoids co-locating use case specific data with unrelated data of the same record type. If applications omit the "-persist" suffix, then they risk collisions with existing underscore scoped labels such as those in the globally scoped underscore labels IANA registry specified by [RFC8552] or existing DCV approaches that have not adopted the "-challenge" suffix defined in [I-D.ietf-dnsop-domain-verification-techniques]. By using the "-persist" suffix, Application Service Providers will also avoid the common pitfalls described in Appendix A.1 of the DCV BCP that may result in avoidable operational impacts [I-D.ietf-dnsop-domain-verification-techniques].

Application Service Providers can also use multiple labels to support additional features using a similar approach as described in [I-D.ietf-dnsop-domain-verification-techniques] but applied to the persistent label, e.g., "_<FEATURE>._<USE_CASE_RELEVANT_NAME>-persist".

2.2. DNSSEC Requirements

Application Service Providers MUST use DNSSEC or its successor ([RFC9364]) and provide mechanisms that ensure only valid DNSSEC signatures covering the expected DNS resource records are accepted for use.

DNSSEC validation failures SHOULD start the process of de-associating a domain name in an Application Service Provider as it relates to a particular use case or trigger processes to re-evaluate the association. How exactly this occurs is left to the Application Service Provider.

The use of DNSSEC is REQUIRED for two reasons. First, it provides for global consistency such that any Application Service Provider that is given a DNSSEC signed record can cryptographically verify its authenticity. Second, DNSSEC mitigates spoofing attacks based on forged response data. Such a spoofing attack could lead to scenarios where a domain name is erroneously associated with another user's application presence. The requirement to perform periodic checks, described in Section 2.3, implies such a spoofing attack will eventually be identified. DNSSEC can reliably prevent the attack in the first place as it relates to forged response data.

It is RECOMMENDED that Application Service Providers provide at least one other method for authenticating persistent references to accommodate domain names for which DNSSEC support for this purpose is not available. This ensures that such domain names have other mechanisms to participate. Non-limiting examples include HTTP-based approaches such as the HTTP-01 ACME challenge or AT Protocol's use of well-known endpoints.

2.3. Periodic Confirmation

Application Service Providers MUST periodically check that any associated domain name is still associated with the use case, e.g., by checking for the presence of the expected DNS record(s) and their DNSSEC signatures. This ensures the Application Service Provider will eventually identify changes that impact the use of the domain name for their use cases.

The frequency of this check will vary by use case and is left to the discretion of the Application Service Provider.

3. Security Considerations

3.1. DNSSEC Signature Validity

DNSSEC signatures have a validity period that includes an inception and expiration timestamp. If two DNSSEC signatures covering an RRset have overlapping validity periods, then both may appear valid during the overlap, e.g., because an old signature has yet to expire. If Application Service Providers are concerned about accepting an older signature, then the Application Service Provider could keep track of the inception time when verifying signatures and only use the most recent RRset and signature encountered. Older, valid signatures could then be rejected which would reduce the risk of replay attacks using the older but still valid data.

3.2. Privacy Considerations

One challenge for users who wish to obscure which use cases a domain name supports is that many use cases require a domain name use a widely known label (e.g., published in open specifications) that any Application Service Provider can access. As a result, anyone with knowledge of that use case will be aware of the label to use to query for data associated with that use case. However, users can mitigate those without knowledge from trivially enumerating the use cases a domain supports using techniques such as NSEC3 [RFC5155] or compact denial of existence [I-D.ietf-dnsop-compact-denial-of-existence] to limit zone walking.

4. IANA Considerations

This document has no IANA actions.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

5.2. Informative References

[I-D.birgelee-lamps-caa-security] Birge-Lee, H., Cimaszewski, G., Kr辰henb端hl, C., Wang, L., Gable, A., and P. Mittal, "CAA Security Tag for

Cryptographically-Constrained Domain Validation", Work in Progress, Internet-Draft, draft-birgelee-lamps-caa-security-02, 21 March 2025, <https://datatracker.ietf.org/doc/html/draft-birgelee-lamps-caa-security-02>.

[I-D.chins-dnsop-web3-wallet-mapping]
Chin, S., "DNS to Web3 Wallet Mapping", Work in Progress, Internet-Draft, draft-chins-dnsop-web3-wallet-mapping-02, 18 February 2025, <https://datatracker.ietf.org/doc/html/draft-chins-dnsop-web3-wallet-mapping-02>.

[I-D.ietf-dnsop-compact-denial-of-existence]
Huque, S., Elmerot, C., and O. Gu丹mundsson, "Compact Denial of Existence in DNSSEC", Work in Progress, Internet-Draft, draft-ietf-dnsop-compact-denial-of-existence-07, 27 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-compact-denial-of-existence-07>.

[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>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC8552] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/info/rfc8552>.

[RFC8659] Hallam-Baker, P., Stradling, R., and J. Hoffman-Andrews, "DNS Certification Authority Authorization (CAA) Resource Record", RFC 8659, DOI 10.17487/RFC8659, November 2019, <https://www.rfc-editor.org/info/rfc8659>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[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>.

[atproto] Bluesky, "Handle", 2025, <https://atproto.com/specs/handle>.

[bip353] Corallo, M. and B. Teinturier, "DNS Payment Instructions", 2024, <https://en.bitcoin.it/wiki/BIP_0353>.

[ens] Ethereum Name Service, "Importing a DNS name", 2025, <https://docs.ens.domains/learn/dns#importing-a-dns-name>.

[walletrr] Hoffman, P., "Public wallet address", 2024, <https://www.iana.org/assignments/dns-parameters/WALLET/wallet-completed-template>.

Appendix A. Survey of Persistent Reference Use Cases

What follows is a brief synopsis of use cases that have been deployed and how they leverage persistent references with a domain name using a DNS-based method.

A.1. Wallet Naming

There are many DNS-based wallet naming mechanisms that have been proposed. The Ethereum Name Service has solutions that uses DNSSEC and TXT records [ens]. The Bitcoin community has BIP-353, a Bitcoin standards track document that uses DNSSEC and TXT records [bip353]. There is also an individual IETF draft [I-D.chins-dnsop-web3-wallet-mapping] which makes use of DNSSEC and both the TXT and WALLET resource record types [walletrr].

Each of these mechanisms can be adopted by individual Application Service Providers, such as wallet applications. Since any number of independent wallet applications may adopt a particular mechanism, there is a desire for such mechanisms to enable multiple Application Service Providers to confirm the association independently to ensure each Application Service Provider can interoperate. In this way, regardless of which wallet application is being used, if it supports a given mechanism it should behave consistently.

A.2. Social Media Handles

The social media handle use case is currently found in decentralized and federated mechanisms such as AT Protocol [atproto]. In AT Protocol, the user's persistent identifier "can be opaque and unfriendly for human use", so associating one with a domain name provides a user friendly identifier to serve as the user's public facing social media handle.

AT Protocol is not an application itself, but a specification that other applications can build on. As such, any Application Service Provider that adopts this mechanism needs to be able to independently confirm the association, e.g., so that every application shows that the same user is associated to the same domain name to avoid the potential for confusion or mis-attribution of information in AT Protocol-based applications.

A.3. CAA Records

CAA records enable a domain name holder to stipulate which Certification Authorities (CA) can issue certifications on their behalf as laid out in [RFC8659]. In this case, the persistent association is the user's intention of who is authorized (or not) to issue certificates which reflects that such associations need not be restricted to a user's identifier in a particular use case.

Appendix B. Change Log

00: Initial draft of the document.

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, VA 20190
Email: ssheth@verisign.com
URI: https://www.verisignlabs.com/

A. Kaizer
Verisign Labs
12061 Bluemont Way
Reston, VA 20190
Email: akaizer@verisign.com
URI: https://www.verisignlabs.com/