Workgroup: Network Working Group
Internet-Draft:
draft-latour-dns-and-digital-trust-02
Published: 11 April 2024
Intended Status: Informational
Expires: 13 October 2024
Authors: J. Carter CIRA
J. Latour CIRA
M. Glaude NorthernBlock

Leveraging DNS in Digital Trust: Credential Exchanges and Trust Registries

Abstract

This memo describes an architecture for trust registry membership association and verification using Decentralized Identifiers (DIDs), trust registries, and the DNS. This architecture provides a verifier with a simple process by which to determine and verify an issuer's membership in a trust registry.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://CIRALabs.github.io/DNS-Based-VCs-and-Trust-Registries-ID/draft-DNS-Based-Digital-Verifiable-Credential-Verification-and-Trust-Registry-Architecture.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-latour-dns-and-digital-trust/.

Source for this draft and an issue tracker can be found at https://github.com/CIRALabs/DNS-Based-VCs-and-Trust-Registries-ID.

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 13 October 2024.

Table of Contents

1. Introduction

This memo aims to demonstrate how trust registries can enable global interoperability by providing a layer of digital trust in the use of digital credentials, demonstrating that trust registries can facilitate a more efficient and trustworthy credential verification process. By leveraging the publicly resolvable and widely supported DNS/DNSSEC infrastructure, entities looking to make a trust decision can easily validate not only the integrity of the credential they are presented with, but also quickly associate the entity in question with a domain name and organization, as well as their authority and trustworthiness by confirming their membership in a trust registry. We will explore how this implementation can present a more decentralized approach to making trust decisions, without

having to integrate directly to all trust registries, but instead letting entities involved in private transactions leverage existing internet infrastructure to facilitate their own trust decisions.

We will focus this memo around a use case involving an individual or an organization receiving a verifiable credential [AnonCreds] [W3C-VC-Data-Model] from an issuer and storing it in their digital wallet. When the individual needs to provide proof of identity or other claims, they present the verifiable credential to a verifier in the form of a verifiable claim which normally includes a digital signature. The verifier then performs several steps to verify the authenticity of the credential, including extracting the issuer's DID from the credential, resolving it according to the corresponding did method to obtain the issuer's DID document, verifying the signature of the credential using the public key in the issuer's DID document, and finally verifying the issuer through a trust registry grounded in the DNS using URI and TLSA records, while ensuring all these DNS records are properly signed and validated with DNSSEC.

This process allows for the secure and decentralized verification of digital credentials in a manner that is transparent and auditable, while also existing alongside and independent of the many different decentralized identity ecosystems and implementations by grounding itself in the DNS.

1.1. Note

The standardization of the various implementations of DIDs, Verifiable Credentials, and more specifically, Trust Registries, is required to to ensure global interoperability of the diverse and emerging digital identity ecosystem.

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.

3. Terminology

* **Issuer**: The source of credentials—every verifiable credential has an issuer. Issuers can include organizations such as government agencies (passports, verified person), financial institutions (credit cards), universities (degrees), corporations (employment IDs), churches (awards), etc. Individuals can issue themselves self-attested credentials - and depending on the governance framework of a digital credentialing ecosystem, individuals could issue credentials to others.

*__Holder__: The recipient of digital credentials. The Holder stores their credentials inside a digital wallet and uses agent technology to interact with other entities. A Holder can be a person, an organization or a machine.

*__Verifier__: A verifier can be anyone seeking trust assurance of some kind about the holder of a credential. Verifiers request the credentials they need and then follow their own policy to verify their authenticity and validity. For example, a TSA agent at an airport will look for specific features of a passport or driver’s license to see if it is valid, then check to ensure it is not expired.

*__Digital Wallet/Agent__: A digital wallet, in the context of digital identity, is a secure platform or application that stores and manages an individual's personal identification and authentication credentials, such as government-issued IDs, passports, driver's licenses, and biometric data in the form of verifiable credentials. The Agent allows the subject to establish unique, confidential, private and authentic channels with other agents.

*__Verifiable Data Registry (VDR)__: A storage location where information relating to Decentralized Identifiers (DIDs) and credential metadata are stored. Permissionless blockchains or permissioned distributed ledger networks can be used to facilitate the discovery and resolution of DIDs and credential information.

*__Trust Registry__: Trust registries are services that help determine the authenticity and authorization of entities in an ecosystem governance framework. They allow governing authorities to specify what actions are authorized for governed parties and enable checking if an issuer is authorized to issue a particular credential type. Essentially, trust registries serve as a trusted source for verifying the legitimacy of credential issuers, wallet apps, and verifiers.

4. The Role of Trust Registries in Bidirectional Credential Verification

A trust registry is a decentralized system that enables the verification of the authenticity and trustworthiness of issuers of digital credentials. Trust registries can be implemented using distributed ledger technology and leverage the DNS to provide a transparent and auditable record of issuer information.

When an entity is presented with a verifiable claim, there are three things they will want to ensure:

1. That a claim hasn’t been altered/falsified at any point in time, via cryptographic verifiability and Verifiable Data Registries (VDRs).

2. That a claim has accurate representation via authentication, via DID Discovery & mapping within DNS as described above.

3. That a claim has authority, or in other words, does the issuer have authority in its issuance of credentials, via the use of trust registries (or trust lists).

In this memo, trust registries enable the verification of the authority of an issuer and by extent their credentials. The role of a trust registry within the context of this document is to confirm the authenticity and trustworthiness of the issuer to the verifier after they have validated the digital credential using the mechanisms described previously. This involves the trust registry taking on the role of a trust anchor for a given ecosystem, providing input for the verifier’s ultimate trust decision regarding the credential they are being presented with. The assumption is made that the trust registry would be operated under the authority of an institution or organization such that their claims and input to the trust decision would be considered significant or definitive. An example of such an organization would be a government entity in relation to the issuance of a driver’s licence.

It is important to note that the DNS based trust registry mechanism described in this section is not meant to operate in place of an alternative implementation but provide an easy to implement and use mechanism to extend such a solution.

This section also does not describe the process of the trust registry’s verification of an issuer, or the process of how an issuer would become accredited by or join a trust registry.

4.1. Issuer's Membership Claim in a Trust Registry

Once a verifier has successfully completed the credential verification process, they have definitive proof that the credential they are being presented with was issued by the claimed issuer. However, this process does not provide definitive proof the issuer is to be trusted or has the authority to issue such a credential. The issuer, through use of URI records and the *_trustregistry* label, can assert the claim that they are a member of a trust registry.

Ex: _trustregistry.example-issuer.ca IN URI 0 1 “example-trustregistry.ca”

This record indicates the verifier can query the *example-trustregistry.ca* DNS based trust registry for TLSA records containing *example-issuer.ca's* public key/s, proving their membership.

4.1.1. URI Record Name Scoping

When trust registry membership claims are published in the DNS

* The records **MUST** be scoped by setting the global (highest-level) underscore name of the URI RRset to *_trustregistry* (0x5F 0x74 0x72 0x75 0x73 0x74 0x72 0x65 0x67 0x69 0x73 0x74 0x72 0x79)

4.2. Trust Registry Membership Proof

The trust registry can assert an issuer's membership using TLSA records.

Ex: _example-issuer.ca._trustregistration.example-trustregistry.ca in TLSA 3 1 0 “4e18ac22c00fb9...b96270a7b6”

Note that the first component of the URI is the issuer’s domain, followed by the *_trustregistration* label. This combination indicates that the domain expressed is registered by this trust registry as per its governance model, and this is their public key. This association created by the TLSA record effectively has created a chain of trust, beginning at the Issuer's public key, continuing to the issuer’s domain, and finally resolving at the Trust Registry.

5. Role of DNSSEC for Assurance and Revocation

It is a **MUST** that all the participants in this digital identity ecosystem enable DNSSEC signing for all the DNS instances they operate. See [RFC9364].

DNSSEC provides cryptographic assurance that the DNS records returned in response to a query are authentic and have not been tampered with. This assurance within the context of the *_did* URI and *_did* TLSA records provides another mechanism to ensure the integrity of the DID and its public keys outside of the distributed ledger it resides on directly from the domain of its owner.

Within this use-case, DNSSEC also provides revocation checks for both DIDs and public keys. In particular, a DNS query for a specific *_did* URI record or *_did* TLSA record can return an NXDOMAIN [RFC8020] response if the DID or public key has been revoked. This approach can simplify the process of verifying the validity of DIDs and public keys by reducing the need for complex revocation mechanisms or implementation specific technologies.

6. Security Considerations

TODO Security

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[alsoKnownAs] "Decentralized Identifiers (DIDs) v1.0", n.d., <https://www.w3.org/TR/did-core/#also-known-as>.

[AnonCreds] "AnonCreds Specification", n.d., <https://hyperledger.github.io/anoncreds-spec/>.

[DID-in-the-DNS] "The Decentralized Identifier (DID) in the DNS", n.d., <https://datatracker.ietf.org/doc/html/draft-mayrhofer-did-dns-05#section-2>.

[DID-Specification-Registries] "DID Specification Registries", n.d., <https://www.w3.org/TR/did-spec-registries/#did-methods>.

[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/rfc/rfc2119>.

[RFC8020] Bortzmeyer, S. and S. Huque, "NXDOMAIN: There Really Is Nothing Underneath", RFC 8020, DOI 10.17487/RFC8020, November 2016, <https://www.rfc-editor.org/rfc/rfc8020>.

[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/rfc/rfc8174>.

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

[services] "Decentralized Identifiers (DIDs) v1.0", n.d., <https://www.w3.org/TR/did-core/#services>.

[verificationMethod] "Decentralized Identifiers (DIDs) v1.0", n.d., <https://www.w3.org/TR/did-core/#verification-methods>.

[W3C-VC-Data-Model] "Verifiable Credentials Data Model v1.1", n.d., <https://www.w3.org/TR/vc-data-model/>.

8.2. Informative References

[Pan-Canadian_Trust_Framework] DIACC, "PCTF Trust Registries Draft Recommendation V1.0 DIACC / PCTF13", n.d., <https://diacc.ca/wp-content/uploads/2023/03/PCTF-Trust-Registries-Component-Overview_Draft-Recomendation-V1.0.pdf>.

[Self-Sovereign_Identity] Reed, D. and A. Preukschat, "Self-Sovereign Identity", ISBN 9781617296598, 2021.

[ToIP_Trust_Registry_Specification] Trust Over IP (ToIP) Working Group, "ToIP Trust Registry Protocol V1 Specification", n.d., <https://github.com/trustoverip/tswg-trust-registry-tf/blob/main/v1/docs/ToIP%20Trust%20Registry%20V1%20Specification.md>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Jesse Carter
CIRA

Email: jesse.carter@cira.ca

Jacques Latour
CIRA

Email: jacques.latour@cira.ca

Mathieu Glaude
NorthernBlock

Email: mathieu@northernblock.io