Verifiable Identifiers

A Best Practice for Decentralized Identifiers (DIDs)

Joe Andrieu joe@legreq.com

Verifiable Identifiers (VID), are a way to use Decentralized Identifiers (DIDs)[1] to provide platform-independent cryptographic verification of actions taken on behalf of that identifier in a flexible, privacy respecting way.

Originally developed as **Interchain Identifiers** (IIDs)[2] to help the Interchain Foundation integrate DIDs with NFTs on the Cosmos platform, VIDs are a particular approach of using DIDs that can be applied with just about any DID method that supports verification relationships and methods. With just a few deisgn choices, any DID method can be used as a VID to get improved semantic rigor, better privacy, and greater interoperability across a range of use cases.

It is worth noting that all VIDs are DIDs, however not all DIDs are VIDs. Yet.

Four key requirements led to **Verifiable Identifiers**: 1. Identifiers that refer to in-registry assets (aka on-chain assets) 2. Identifiers that link in-registry assets to off-registry resources (aka off-chain resources) with a. verifiability that the resource ultimately retrieved is the correct resource b. flexible privacy options c. distinction between semantic references and downloadable resources d. their own verification relationships 3. Identifiers that self-describe 4. Identifiers that support any compatible decentralized system as registry

The **first requirement** was the primary catalyst for IIDs. We needed to be able to use a DID to refer to NFTs in the Cosmos ecosystem, to point to a specific on-chain asset unambiguously and verifiably. For example, we wanted a DID that points to a specific Crypto Kitty or Bored Ape.

Requirement 1 is satisfied by interpreting all VIDs as referring to the in-registry control asset. Since DIDs can point to anything, this rule specifies VIDs as a subset of DIDs which have this trait: the subject is the in-registry asset that controls the DID document. By convention, ALL verifiable identifiers' primary subject is the control asset within the method's Verifiable Data Registry (VDR). That is, the subject of the DID/VID is ALWAYS the control asset. VIDs point to a VDR record.

The **second requirement** was needed for flexible meta-data for NFTs.

In some cases, NFTs simply define a URL to download the image of that NFT. In other cases, it is important to specify the creator of the NFT or a real-world event or property that might be related, such as a NFT as a ticket to an event. In other cases, it was vital to have a verifiable link to multiple pieces of evidence related to the minting of that NFT. Rather than just providing a URL that SHOULD return the correct resource, **verifiability** means providing a way to make sure the resource you get is the right one.

We also needed flexible **privacy** options. Several NFT projects currently store the artist's name on-chain, a potentially irrevocable GDPR violation thanks to the vaunted "immutability" feature of most VDRs (because most VDRs are blockchains). In some cases, it is appropriate to store related resources directly in the VDR and represent them directly in the DID document. In other cases, layers of indirection are preferred, enabling the resource to be deletable and privacy-restricted when necessary.

We saw an opportunity to distinguish between identifiers used to download specific digital resources versus identifiers used to refer to subjects in semantic statements, for example in RDF triples. The **HTTPRange14**[3] problem–created by the use of URLs as both identifiers and dereferencable pointers–is resolved to some degree with the VID approach.

Finally, we saw an advantage in specifying **verification relationships** for associated resources, extending the verifiability of VIDs beyond the primary identifier to secondary resources. Today most verifiers will only use the base did for verification relationships. VIDs extends that to allow DID-URLs to specify any verification relationship, including authentication and attestation, for resources separate from that used for the base DID.

Requirement 2 and all of its sub-requirements are satisfied by using a new property, **linkedResource**, which links specific DID URLs to specific semantic references and downloadable resources. DID URLs augment a base DID, e.g., `did:example:abc` with path, query, or fragment parts, these augmented DIDs are called DID URLs.

VIDs with a path part, e.g., `did:example:abc/image.png` are called VID resources, and are used to point to downloadable resources. The means for dereferencing these resources is contained in their linkedResource entry.

VIDs with a fragment part, e.g., `did:example:abc#creator` are called VID references, and are used to refer to subjects in the context of that VID, allowing statements about those subjects, e.g, in Verifiable Credentials or in the DID document.

For example, the DID controller could define a verification relationship for an asset creator, identified with **#creator** with a JSON snippet like this

```
{
    ...
    "linkedResource" : [{
        "id" : "#creator",
        "authentication" : [{
            "id": "did:example:abc#keys-creator-2",
            "type": "Ed25519VerificationKey2020",
            "controller": "did:example:abc#creator",
            "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
        }]
```

```
    }]
}
```

This approach supports the DID document as a controller specifying how to verify authentication actions taken on behalf of `did:example:abc#creator`.

Requirement 3 deals with the usability of identifiers out of context. Many references to on-chain assets today depend on knowing which decentralized system is meant. This has led to problems with accidental transfer of crypto assets because the same identifier could be used for multiple different blockchains. When the identifier itself defines which registry contains the control asset, we avoid this problem.

Requirement 4 acknowledges the fundamental nature of decentralized technology: to be truly decentralized, the identifiers themselves must be usable without ambiguity with any system that can support them.

The **third and fourth requirements** are satisfied by using DIDs. DIDs are self-describing and work with any data registry through the definition of methods specific to each registry.

Past Work

1. https://w3id.org/earth/Identifiers The IID specification
2. https://internft.org The InterNFT work initially sponsored by the Interchain Foundation
3. https://github.com/interNFT Repo for the InterNFT work

Future Work

I'd like to work with fellow attendees of Rebooting the Web of Trust to tease out the details of a proper specification for VIDs, including a specification suitable for registering new properties with the W3C DID Specification Registries.

I'll maintain this work on VerifiableIdentifiers.org until such a time as it is appropriate to move to a more open, collaborative workspace.

http://verifiableidentifiers.org

References

[1] Decentralized Identifiers (DIDs) https://w3.org/tr/did-core July 19, 2022, Accessed Sep 15, 2022

[2] Interchain Identifiers (IIDs) https://w3id.org/earth/Identifiers Oct 14, 202, Accessed Sep 15, 2022

[3] HTTPRange14 https://en.wikipedia.org/wiki/HTTPRange-14 Accessed Sep 15, 2022