Exploring Decentralized Digital Identity Protocols

Kaliya Young, Identity Woman

IRTF DINRG July, 24 2024
Kaliya Young

Co-Founder
Co-Producer
Co-Facilitator

Founding Partner

We provide consulting and advisory services to help governments, industries and organizations globally transition to the new generation of decentralized identity infrastructure.

OpenID and OAuth were founded at IIW

Rest of this talks what we have innovated in the last 10 years.
Exploring Decentralized Digital Identity Protocols

1. Decentralized Identifiers
2. Verifiable Credentials
3. Exchange Protocols
4. Decentralized Trust & Governance Frameworks
5. Where work is happening
Decentralized Identifiers

Approved by W3C v 1.1

New Maintenance Working Group
+ mandate to specify resolution
How are digital identifiers managed today?
Private Name Spaces

Identifiers in privately controlled namespaces
Private Name Spaces

• At the Affect of the owner of the namespace
• Often only communicate internal to namespace
  • With exception of e-mail (open standard) to communicate across domains
Globally Managed Registries

Identifiers in globally managed hierarchical name spaces.
Globally Managed Registries

• Broadly Accessible
• Pay rent to keep your “identifier”
• At the affect of / governance of the names space
• Globally Resolvable
• Basis of global communications networks
• But have emerging security and fraud concerns
How are Decentralized Identifiers Different?

• Any Entity can create one
  • Using software they control

• Infinitely large namespace
Decentralized Identifier (DID)

```
did:method:3k9dg356wdcj5gf2k9bw8kfg7a
```

“Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.”

(Source: https://www.w3.org/TR/did-core/)
Decentralized Identifier (DID)

```
c2cd0ffde594d278c2d9b432f4748506a7f
9f25141e485eb84bc188382019b6
```

Public Key

did:method:4EFNaYeA9hDp6F55JAB38EftNcYEbbM9nwK

Private Key

```
047d599d4521480d9e1919481b024f29d
2693f272d19473dbef971d7d529f6e9
```
Decentralized Identifier (DID)

{ "Key": "Value" }

DID

Decentralized Identifier

DID Document

JSON-LD document describing the entity identified by the DID
Decentralized Identifier (DID)

The standard elements of a DID doc

1. **DID** (for self-description)

2. **Set of public keys** (for verification)

3. **Set of auth protocols** (for authentication)

4. **Set of service endpoints** (for interaction)

5. **Timestamp** (for audit history)

6. **Signature** (for integrity)
"created": "2002-10-10T17:00:00Z",
"updated": "2016-10-17T02:41:00Z",
"signature": {
  "type": "Rsasignature2016",
  "created": "2016-02-08T16:02:20Z",
  "creator": "did:sov:8uQhQMGzWxr8vw5P3UWH1j#key/1",
  "signatureValue": "IOmA4R7TfhkYTYW87z64003GYF1dw0yqie9Wl1kZ5OBYNAK0wG5u0sPRK8/2C4STOWF+83cmcbZ3CBMq2/gi25s="
}
}
Decentralized IDentifier - DID

Verifiable Data Registry

- DID subject
  - identifies DID

- DID controller
  - can modify DID document

- DID
  - recorded on DID URL
  - generates DID method
  - resolves to DID resolver
  - dereferences to resources like public keys, service endpoints, etc.

- DID resolver
  - instructs
  - (resolving and dereferencing)
In the Reality and Spirit of Decentralization

The DID standard doesn’t define “A DID” method but a kind of MVP for a DID method

There is a Registry of DID methods

(Anyone can add to it)

There are over 180 methods!
A DID Method spec defines...

1. The syntax of the method-specific identifier
2. Any method-specific elements of a DID document
3. The CRUD (Create, Read, Update, Delete) operations on DIDs and DID documents for the target system

Slide credit: Drummond Reed, Sovrin Foundation
Many DIDs are Globally Resolvable

- Some DID methods anchor DIDs to public blockchains
- Some are on existing infrastructure like DID Web method into existing DNS
Many DIDs are Globally Resolvable

**DID:Web** (public) supports leveraging existing DNS architecture to anchor DIDs. This provides backwards compatibility into conventional Web 1 and Web 2.0 infrastructure.

**DID:PKH** (public) leverages existing crypto addresses to create DIDs. It allows most if not all blockchain accounts to instantly leverage an existing identity/account and deploy a DID from it in a standards-conformant way. This provides forward compatibility into Web 3.0 infrastructure.

**DID:TDW** (public) Trust DID Web is an enhancement to the DID method. Including a self-certifying identifier (SCID) for the DID that is globally unique, embedded in the DID, and derived from the initial DIDDoc.
Maintains Code for a Universal Resolver in GitHub

There are companies like Danube Tech that have commercial services for this.

godaddy is a hosted platform that makes it easy for developers and solution providers to work with Decentralized Identity.
Some DIDs are Non-Public

- **DID:PEER** (non-public) is suitable for most private relationships between people, organizations, and things. They create the conditions for people, organizations and things to have full control of their end of the digital relationships they sustain.

- **DID:KEY** (non-public) is used to express public keys in a way that doesn't require a DID Registry of any kind. It is an offline-friendly, cryptographically self-certifying method that requires no trust of certificate authorities or blockchain and is ideal for ephemeral use.
DIDs are Identifiers that are

- Globally resolvable
- Decentralized
- Have Associated
  - Public Keys
  - End Points

Resolvable Decentralized Public Key Infrastructure
DIDs are Deep Infrastructure

Essential to reset the foundation to get beyond:

Private Name Spaces

Globally Managed Registries
Who cares about really long numbers?
Verifiable Credentials

Originally incubated in the Credentials Community Group then Standardized at the W3C

Version 1.1. [Implementors Guide]
Version 2 is nearing completion

**The SPICE working group was just spun up in IETF**

I co-authored a report about the various flavors of digital credentials.
Verifiable Credential (VC)
Who is the Issuer of this credential? e.g. did:web:www.uscis.gov:green-card

What is the current status of this credential? https://w3c-ccg.github.io/vc-status-list-2021/

Who is the Subject of the credential? BYO-W3C-DID

What does the Issuer assert about the Subject? https://w3c-ccg.github.io/citizenship-vocab/

How can a Verifier find the Public Key of the Issuer to Verify the Digital Signature that ensures the integrity and provenance of the credential?
Verifiable Credential (VC)

Broad Expressive Capacity

Huge Range of Use-Cases
Exchange Protocols:

DIDComm

OpenID4VC

OpenIDIDComm
DIDComm Messaging

DIDComm Protocols for Human Communication allow for the interactions between two parties using human focused communication.

DIDComm uses DIDs (Decentralized Identifiers) to establish confidential, ongoing connections, without the need for usernames and passwords.

DIDComm protocols enable trusted interactions between parties. These support activities like secure chat, verifiable credential exchange, buying and selling, scheduling, escrow, bidding, ticketing, and so forth. If not already in use, protocols can be designed for any use case.

Decentralized Identity Foundation Specification on GitHub
DIDComm Messaging

**DID:PEER** (non-public) is suitable for most private relationships between people, organizations, and things. They create the conditions for people, organizations and things to have full control of their end of the digital relationships they sustain.
DIDComm Messaging

Alice and Bob exchange Peer DIDs to create a relationship
DIDComm Messaging
DIDComm & Verifiable Credentials

Private Pairwise Peer DIDs

Issuer

100% OFF-CHAIN

Verifier

Fully GDPR Compliant

DID

Public Key

Verifiable Data Registry (e.g., Blockchain)

To understand OpenID4VC, it is helpful to first understand OAuth 2.0, which is the basis of our work, for a brief overview, just have a look at [OAuth 2.0 simplified](#).

**OID4VCI** is used for the issuance of Verifiable Credentials. It provides an API:

- Credential Endpoint
- Batch Credential Endpoint
- Deferred Credential Endpoint

**OpenID4VP** is used for the presentation of Verifiable Credentials. It extends the OAuth2.0 flow by introducing the so called VP Token as a container which allows users to present their presentations to verifiers via a wallet. One can distinguish different scenarios where the verifier and the user are using the same device (Same-Device-Flow) or using different devices (Cross-Device-Flow).
OpenID 4 Verifiable Credentials Issuance

Credential issuance via simple OAuth-authorized API

1. Wallet requests & User authorizes credential issuance
2. Wallet requests credential issuance
3. Credential is issued
OpenID4VC

OpenID for Verifiable Presentations

1. User tries to access a resource
2. WP requests Credential(s)*
3. Wallet returns Verifiable Presentation(s) in VP Token

- Query language to granularly specify what kind of credential Verifier wants. (utilizes DIF Presentation Exchange 2.0)
- Verifiable Presentations* are returned in a newly defined VP Token
- Simple overall architecture, e.g., device local communication when same device flow is used
OpenIDIDComm

In order to turn an OID4VC interaction into a DIDComm connection, the OID4VC exchange must include a DID that contains a DIDComm service endpoint, or can be updated to include a DIDComm Service Endpoint. Ideally, both parties share their DID in the exchange, allowing either to initiate a DIDComm relationship.

https://github.com/IDUnion/OpenIDIDComm

https://book.didcomm.org/oid4vc/
Decentralized Trust & Governance Frameworks
What is Governance Framework or Trust Registry?

What types of entity are in the registry?
How do you know who owns Public Keys (DID/x509)?
What types of credentials do they issue?
How is the registry governed?
What do they agree to?

Introduction to Trust Over IP Model

Trust over IP Deliverables Page - Lots of Document
How the Trust Registry fits in with VC exchange
How do you figure out where the Registries Are?

TRAIN (TRust mAnagement INfrastructure)

Image Source: Good Health Pass Interoperability Blueprint page 104

https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/
Regi-Trust is building a directory of trust Registries

Digital TRUST Infrastructure for Discovery and Validation (Regi-TRUST) is an infrastructure project sponsored and hosted at the United Nations Development Programme (UNDP). The project is intended to develop and provide a suite of tools to enable discovery and validation of trusted services by leveraging existing Internet infrastructures of the Domain Name System (DNS) and its security extensions.

Regi-TRUST can enable scalable 'network of networks' model that today’s fully centralized model is not able to. Decentralized, cloud-agnostic architecture it adopts, any participating service of an implemented network or ecosystem will be able to maintain the sovereignty and control of their own systems and data. Such an approach provides the necessary trust infrastructure that can help to thwart the ubiquitous phishing attempts mimicking online service organizations, such as government institutions, health providers and banks.

GitHub Code
Three Centers of Gravity all doing key work on Decentralized ID Standards

Credentials Community Group
https://w3c-ccg.github.io/

Decentralized Identity Foundation
https://decentralized-id.com/

Trust Over IP Foundation
https://trustoverip.org/
Internet Identity Workshop #39
Mountain View, California
October 29-31, 2024

Internet Identity Workshop #40
Mountain View, California
April 6-8, 2025

Regional Events:
DID UnConf Africa
Cape Town South Africa
September 25-27, 2024

APAC Digital Identity unConference
Bangkok, Thailand
January 22-24

Digital Identity unConference Europe
Hack/Write Event in Feb/March 2025
Main Conference: September 2025

https://internetidentityworkshop.com/
Kaliya Young

kaliya@identitywoman.net

consulting.identitywoman.net