

# FUTURE OF THE WEB

Who is managing your privacy  
and identity on the web?

Melbourne: 14 February

Sydney: 21 February

Canberra: 22 February



Australian  
National  
University

## Returning to Online Privacy

Grant Noble  
grant.noble@consensys.net  
Melbourne

Dr. David Hyland-Wood  
david.wood@consensys.net  
Sydney, Canberra

# What do we mean by Credential?

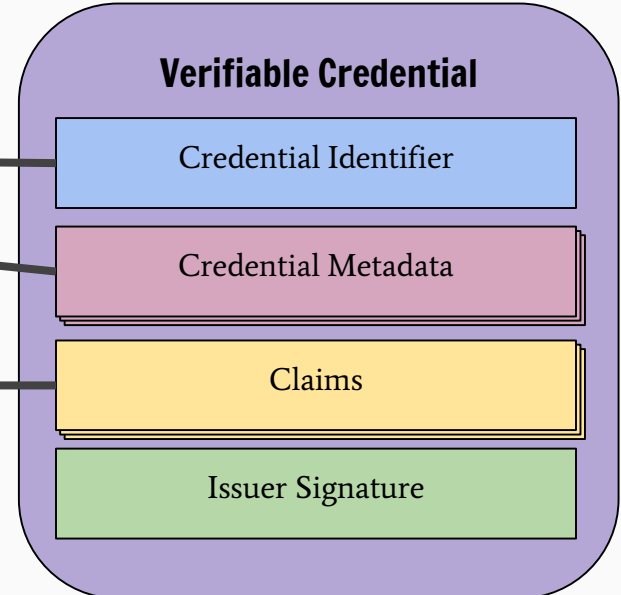


# W3C Verifiable Credentials

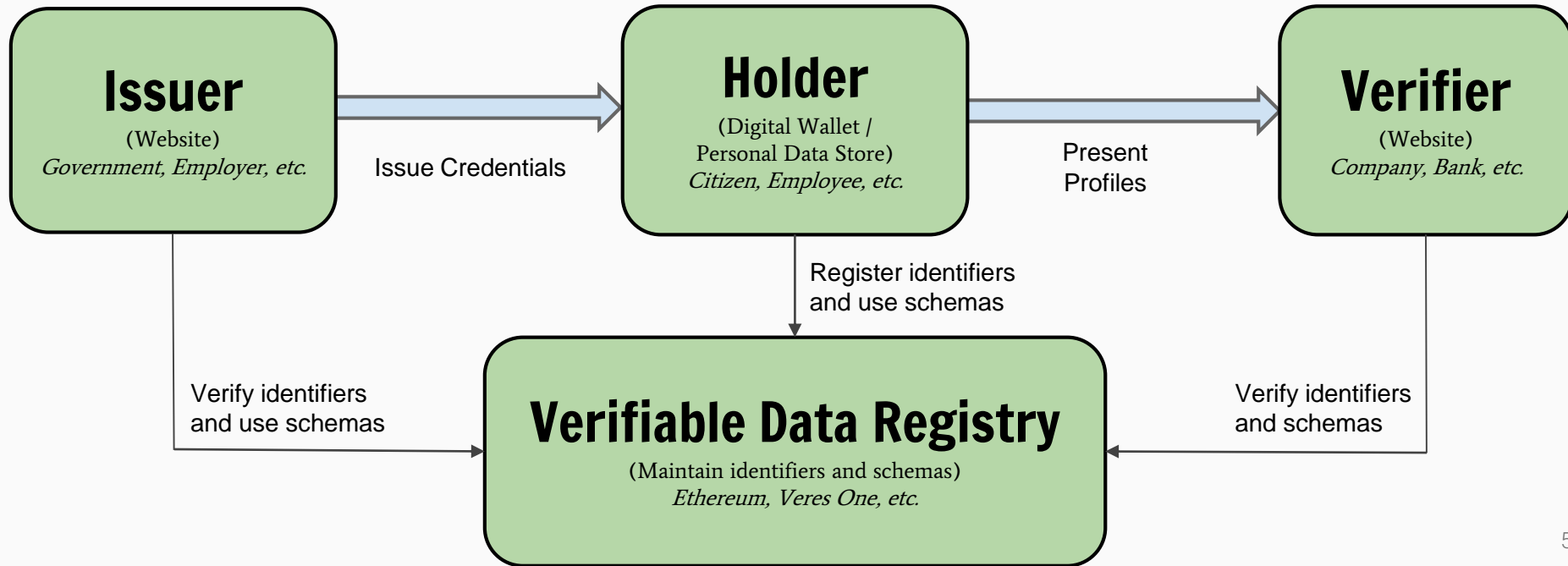
The mission of the W3C Verifiable Credentials Working Group:

*Express credentials on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.*

# Anatomy of a Verifiable Credential



# Verifiable Credentials Ecosystem



- 1. Introduction
  - 1.1 What is a Verifiable Credential?
  - 1.2 Ecosystem Overview
  - 1.3 Use Cases and Requirements
- 2. Terminology
- 3. Core Data Model
  - 3.1 Claims
  - 3.2 Credentials
  - 3.3 Presentations
- 4. Trust Model
- 5. Conformance
- 6. Basic Concepts
  - 6.1 Contexts
  - 6.2 Identifiers
  - 6.3 Types
  - 6.4 Issuer
  - 6.5 Proofs (Signatures)
  - 6.6 Expiration
  - 6.7 Status
  - 6.8 Presentations
- 7. Advanced Concepts
  - 7.1 Extensibility
  - 7.2 Data Schemas
  - 7.3 Refreshing
  - 7.4 Mode of Operation
  - 7.5 Terms of Use
  - 7.6 Evidence
  - 7.7 Zero-Knowledge Proofs
  - 7.8 Subject-Holder Relationships
  - 7.9 Disputes
  - 7.10 Authorization
  - 7.11 Syntactic Sugar
- 8. Syntaxes
  - 8.1 JSON
  - 8.2 JSON-LD
  - 8.3 JSON Web Token
- 9. Verification
  - 9.1 Syntax
  - 9.2 Credential
  - 9.3 Issuer

# Verifiable Credentials Data Model 1.0

Expressing verifiable information on the Web



W3C Editor's Draft 22 January 2019

## This version:

<https://w3c.github.io/vc-data-model/>

## Latest published version:

<https://www.w3.org/TR/vc-data-model/>

## Latest editor's draft:

<https://w3c.github.io/vc-data-model/>

## Editors:

[Manu Sporny \(Digital Bazaar\)](#)

[Gregg Kollogg \(Spec-Ops\)](#)

[Grant Noble \(ConsenSys\)](#)

[Daniel C. Burnett \(ConsenSys\)](#)

[Dave Longley \(Digital Bazaar\)](#)

## Authors:

[Manu Sporny \(Digital Bazaar\)](#)

[Dave Longley \(Digital Bazaar\)](#)

[David Chadwick \(University of Kent\)](#)

## Participate:

[GitHub w3c/vc-data-model](#)

[File a bug](#)

[Commit history](#)

[Pull requests](#)

Copyright © 2019 W3C<sup>®</sup> (MIT, ERCIM, Keio, Beihang). W3C<sup>®</sup> logo, trademark and permissive document license rules apply.

## Abstract

Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable.

## Status of This Document

*This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publications and the latest revision of this technical report can be found in the [W3C technical reports index](https://www.w3.org/TR/) at <https://www.w3.org/TR/>.*

Comments regarding this document are welcome. Please file issues directly on [GitHub](#), or send them to [public-vc-comments@w3.org](mailto:public-vc-comments@w3.org) ([subscribe](#), [archives](#)).

# Verifiable Credentials Status

## Roadmap



Weekly WG Participants: **20-22 / 85**

Spec/Issue Regular Contributors: **15**

Known Corporate Implementation Commitments: **10**

# Questions about Verifiable Credentials?



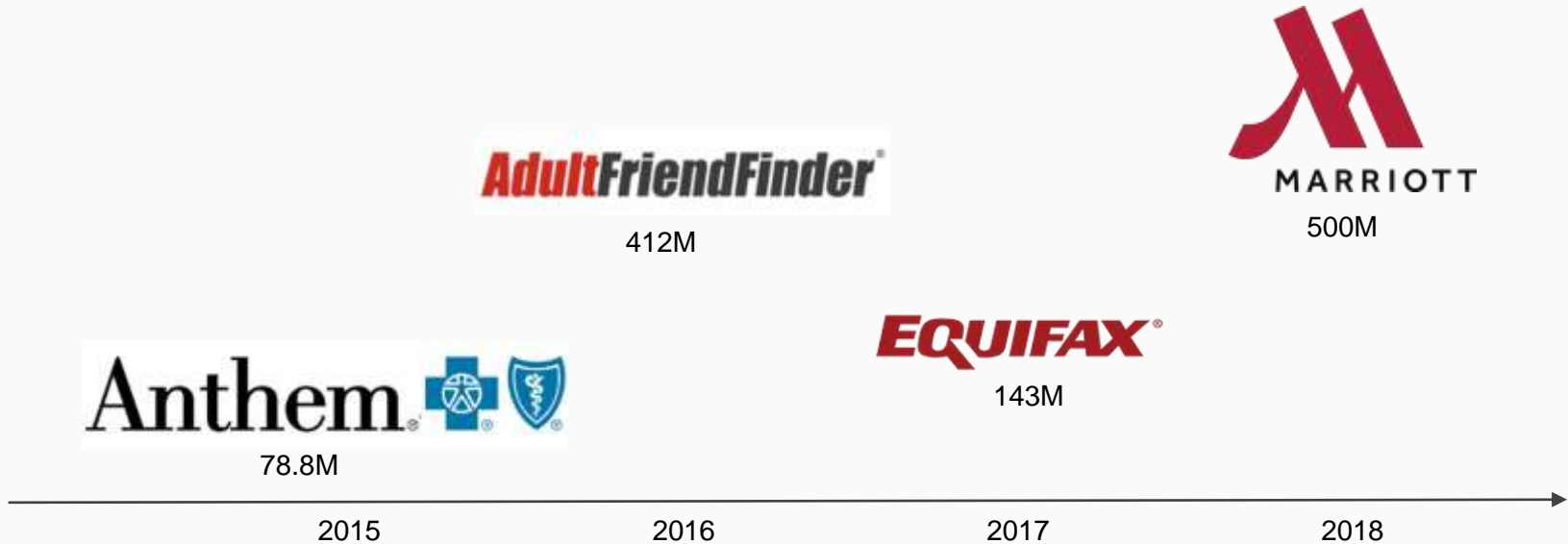
# Which identifiers do we use today?



*jdoe@bigcorp.com*

*https://flitter.com/jdoe*

# Why is this a problem?

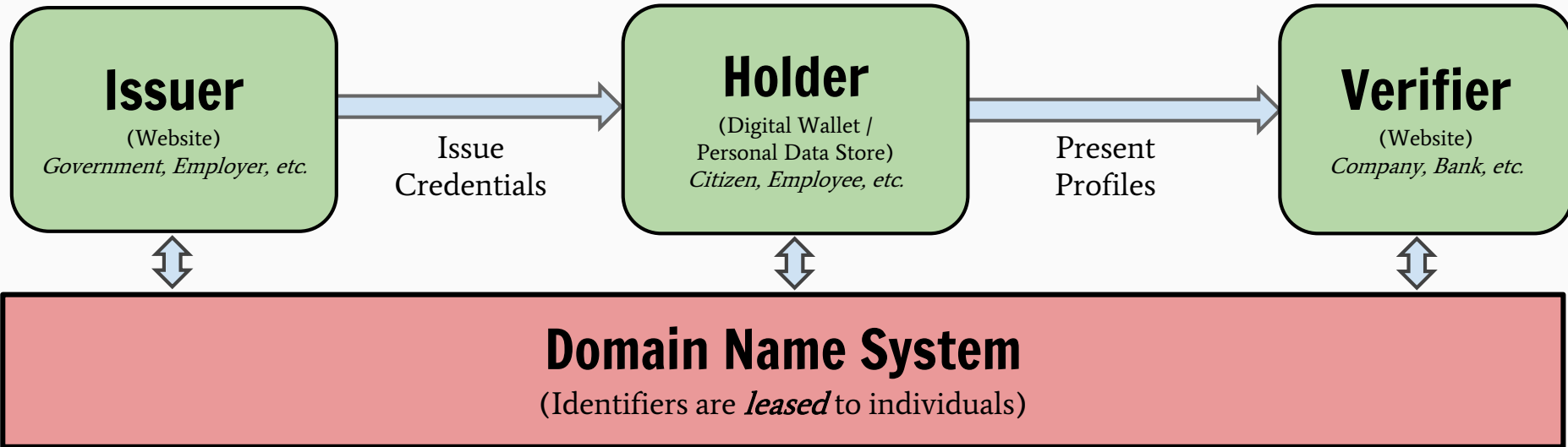


# The Web's Identifier Problem

To date, **no identifier** you use online belongs to you; it belongs to someone else.

*This results in problems related to cost, data portability, data privacy, and data security.*

# Web Identifiers Today



# What is missing?

Many portable identifiers for any person, organization, or thing that does not depend on a centralized authority, are protected by cryptography, and enable privacy and data portability.

# Decentralized Identifiers

A new type of globally resolvable, cryptographically-verifiable identifier, registered directly on a distributed ledger (e.g. a blockchain)

# What does a DID look like?

Diagram illustrating the structure of a DID (Decentralized Identifier):

`did:example:123456789abcdefghijklmnopq`

The structure is defined by brackets:

- `did` is labeled as the **Scheme**.
- `example` is labeled as the **DID Method**.
- `123456789abcdefghijklmnopq` is labeled as the **DID Method Specific String**.

Example:

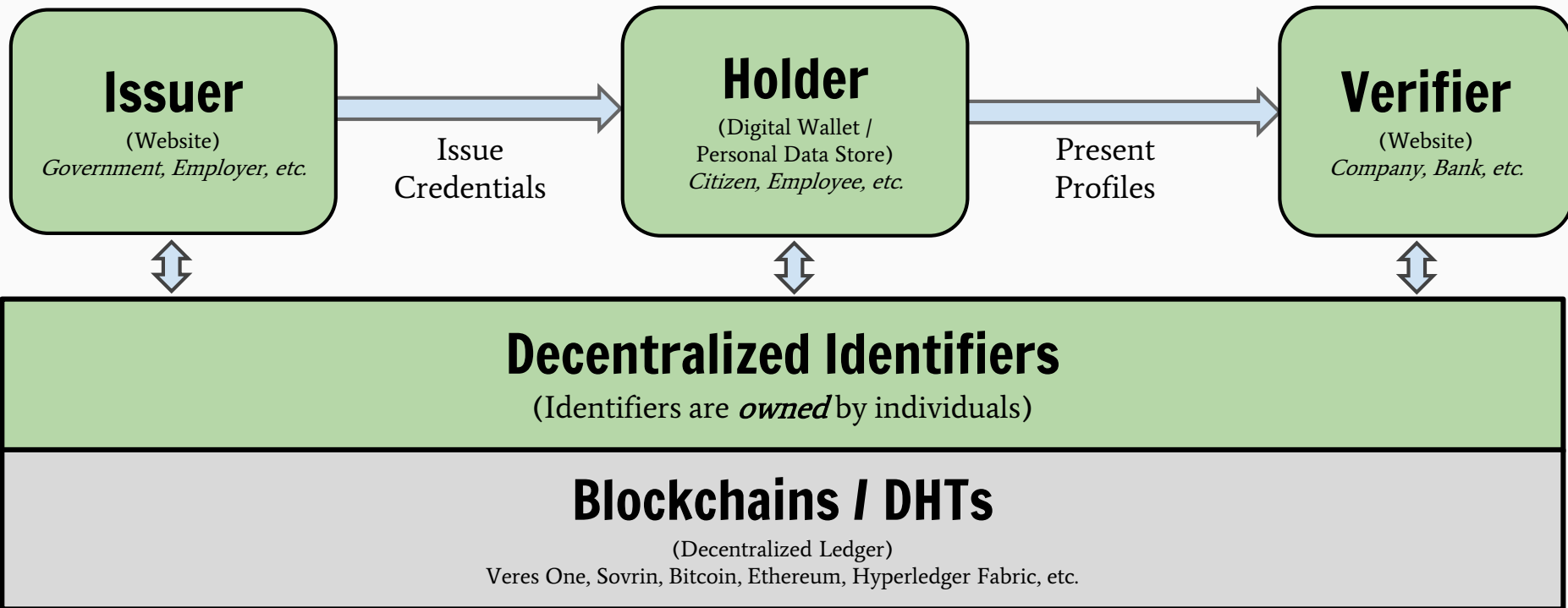
`did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD`

# DIDs Resolve to DID Documents

```
{
  "@context": "https://w3id.org/veres-one/v1",
  "id":
  "did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
  "authentication": [{ ← 1. Authentication Mechanisms
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [{
      "id":
      "did:v1:test:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD#aut
      hn-key-1",
      "type": "Ed25519VerificationKey2018",
      "owner":
      "did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
      "publicKeyBase58": ← 2. Public Key Material
      "DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD"
    }
  ]
},
  "service": [{ ← 3. Service Discovery
    "type": "ExampleMessagingService",
    "serviceEndpoint": "https://example.com/services/messages"
  ]
},
  ... more DID-specific information here ...
}
```



# Decentralized Identifiers



# Decentralized Identifiers (DIDs) v0.11

Data Model and Syntaxes for Decentralized Identifiers (DIDs)



Draft Community Group Report 22 January 2019

## TABLE OF CONTENTS

- 1. Introduction**
  - 1.1 Overview
    - 1.1.1 URIs, URLs, and URNs
    - 1.1.2 Motivations for DIDs
    - 1.1.3 The Role of Human-Friendly Identifiers
    - 1.1.4 Purpose of This Specification
  - 1.2 Design Goals
  - 1.3 Simple Examples
    - 1.3.1 Self-Managed DID Document
- 2. Terminology**
  - 2.1 Base Specifications
- 3. Decentralized Identifiers (DIDs)**
  - 3.1 The Generic DID Scheme
  - 3.2 Specific DID Method Schemes
  - 3.3 Paths
  - 3.4 Fragments
  - 3.5 Normalization
  - 3.6 Persistence
- 4. DID Documents**
  - 4.1 Context
  - 4.2 DID Subject
  - 4.3 Public Keys
  - 4.4 Authentication
  - 4.5 Authorization and Delegation
  - 4.6 Service Endpoints
  - 4.7 Created (Optional)
  - 4.8 Updated (Optional)
  - 4.9 Proof (Optional)
  - 4.10 Extensibility
- 5. DID Operations**
  - 5.1 Create
  - 5.2 Read/Verify
  - 5.3 Update
  - 5.4 Delete/Revoke
- 6. DID Resolvers**

### Latest editor's draft:

<https://w3c-cg.github.io/did-spec/>

### Editors:

[Drummond Reed \(Evernym\)](#)  
[Manu Sporny \(Digital Bazaar\)](#)

### Authors:

[Drummond Reed \(Evernym\)](#)  
[Manu Sporny \(Digital Bazaar\)](#)  
[Dave Longley \(Digital Bazaar\)](#)  
[Christopher Allen \(Blockstream\)](#)  
[Ryan Grant](#)  
[Markus Sabadello \(Danube Tech\)](#)

### Participate:

[GitHub w3c-cg/did-spec](#)  
[File a bug](#)  
[Commit history](#)  
[Pull requests](#)

Copyright © 2019 by the Contributors to the Decentralized Identifiers (DIDs) v0.11 Specification, published by the Credentials Community Group under the [W3C Community Contributor License Agreement \(CLA\)](#). A human-readable [summary](#) is available.

## Abstract

Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URIs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate as the DID subject (e.g., public keys, pseudonymous biometric protocols, etc.). Service endpoints enable trusted interactions with the DID subject.

This document specifies a common data model, format, and operations that all DIDs support.

## Status of This Document

This specification was published by the [Credentials Community Group](#). It is not a W3C Standard nor is it on the W3C Standards Track. Please note that under the [W3C Community Contributor License Agreement \(CLA\)](#) there is a limited opt-out and other conditions apply. [Learn more about W3C Community and Business Groups.](#)

# Decentralized Identifiers Status

## Roadmap



Weekly Community Group Participants: **15-28 / 161**

Spec/Issue Regular Contributors: **12**

Known Corporate Implementation Commitments: **13**

# Questions about Decentralized Identifiers?

# Acknowledgments

- Manu Sporny, CEO at Digital Bazaar
  - Co-Inventor of Verifiable Credentials, Decentralized Identifiers, and JSON-LD
  - 10+ Years in Web Standards
  - msporny@digitalbazaar.com
- Dan Burnett, Standards Champion at ConsenSys
  - Co-chair of the Verifiable Credentials Working Group
  - 20 Years in Web Standards
  - Participant in the Credentials Community Group (Decentralized Identifiers)



# Trademark Attribution

The corporate logos used in this presentation are the registered trademarks of their respective companies.

Logos are used for educational purposes only under fair use provisions of copyright law.