Returning to Online Privacy

Grant Noble
grant.noble@consensys.net
Melbourne

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

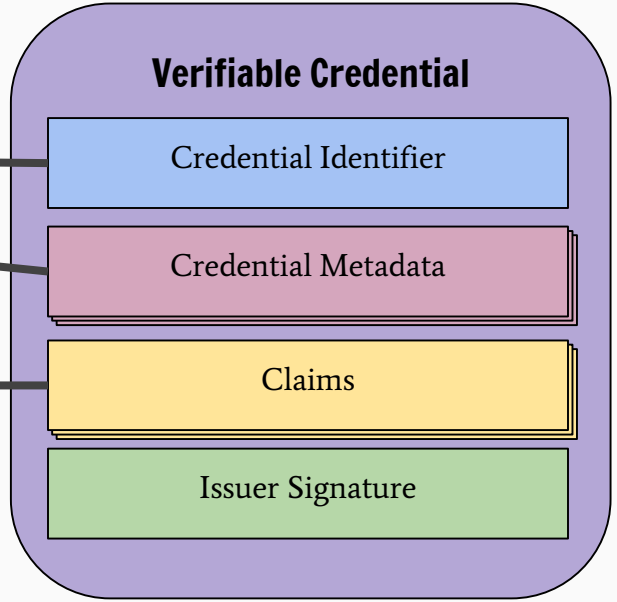
What do we mean by Credential?

W3C Verifiable Credentials

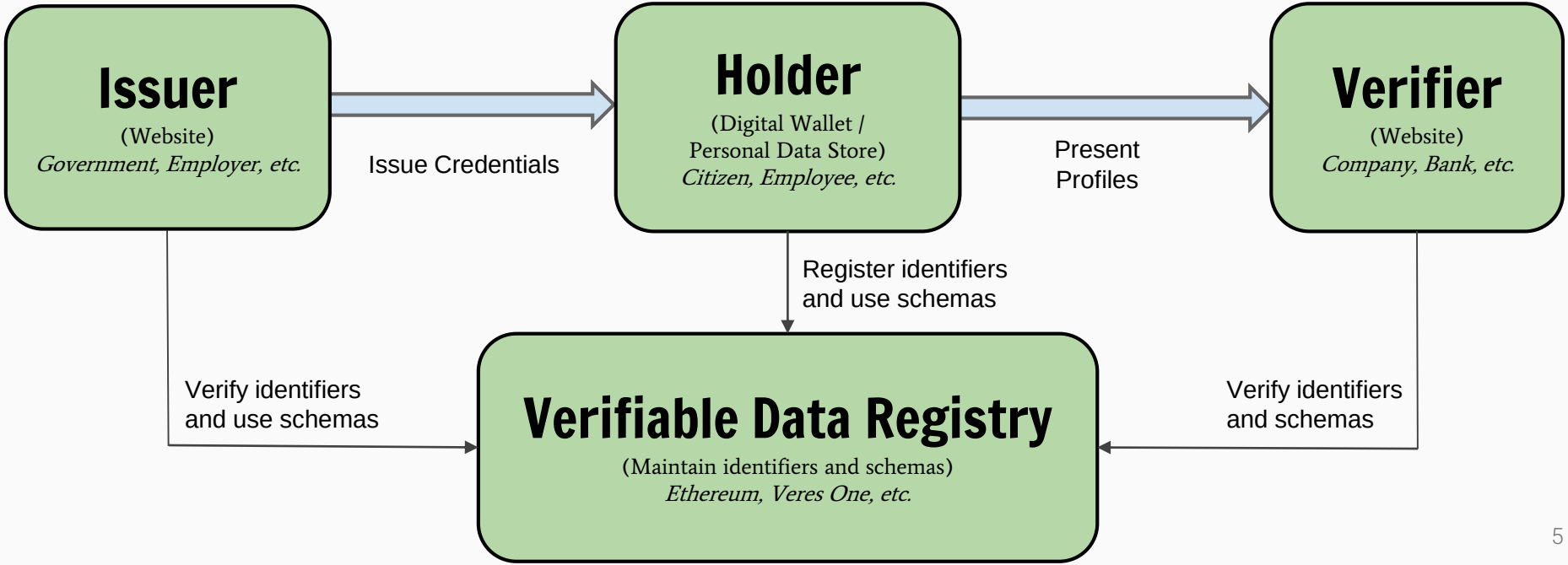
The mission of the W3C Verifiable Credentials Working Group:

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



W3C Editor's Draft

TABLE OF CONTENTS

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 Kellogg (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

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 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 (subscribe, archives).

Verifiable Credentials Status

Roadmap

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

Spec/Issue Regular Contributors: **15**

Known Corporate Implementation Commitments: **10**

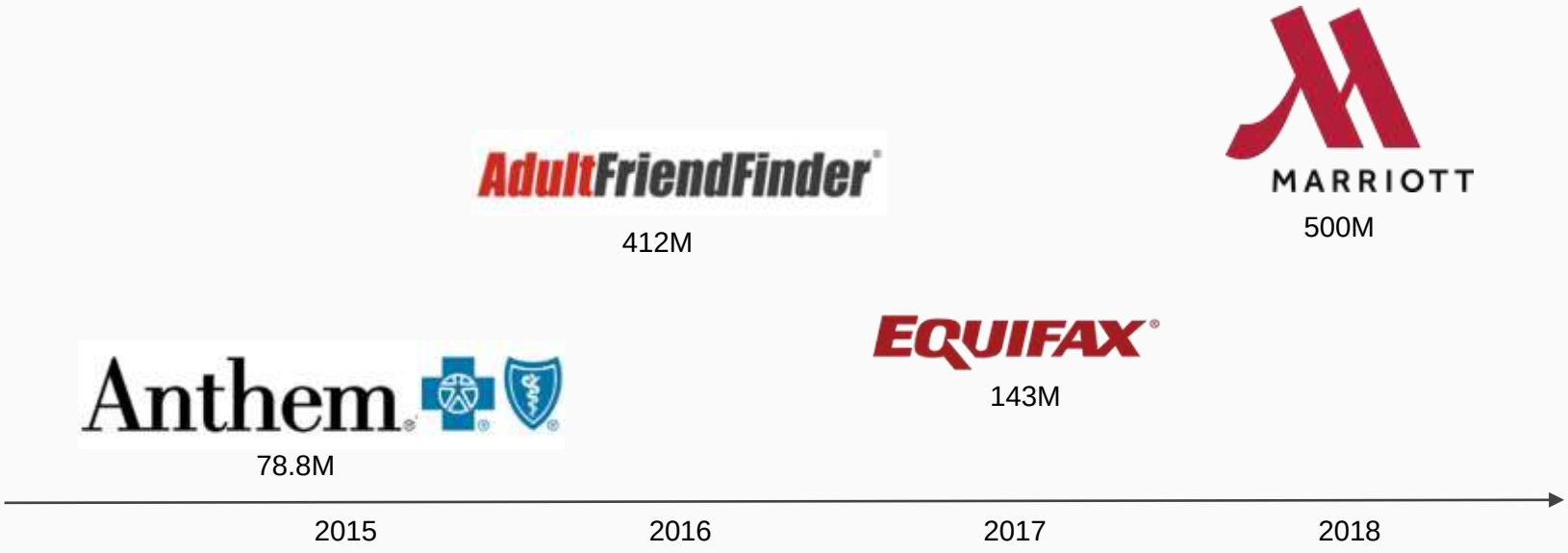
Questions about Verifiable Credentials?

Which identifiers do we use today?

jdoe@bigcorp.com

https://flitter.com/jdoe

Why is this a problem?

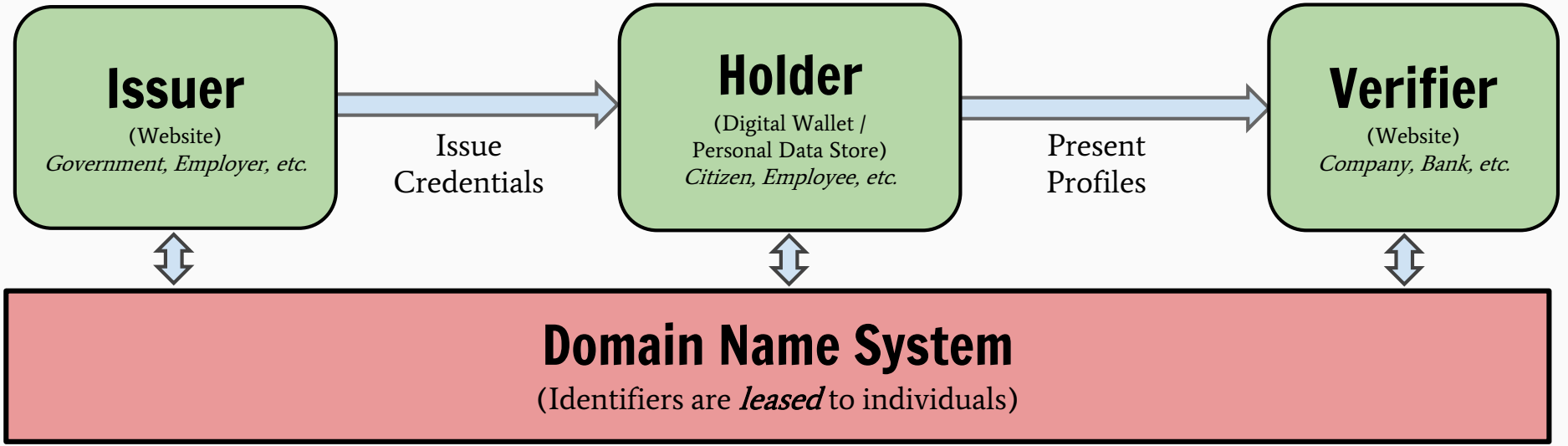


The Web's Identifier Problem

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



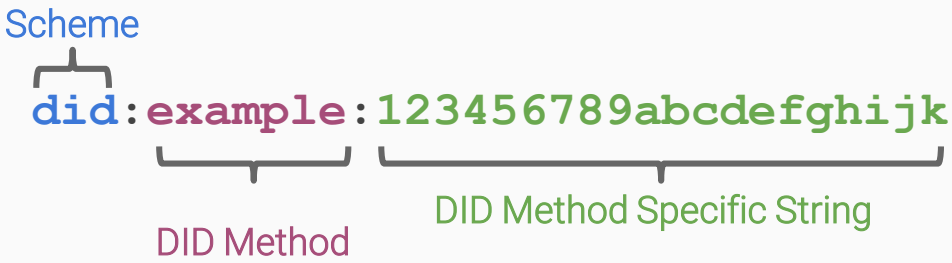
What is missing?

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?



Example:

did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD

DIDs Resolve to DID Documents

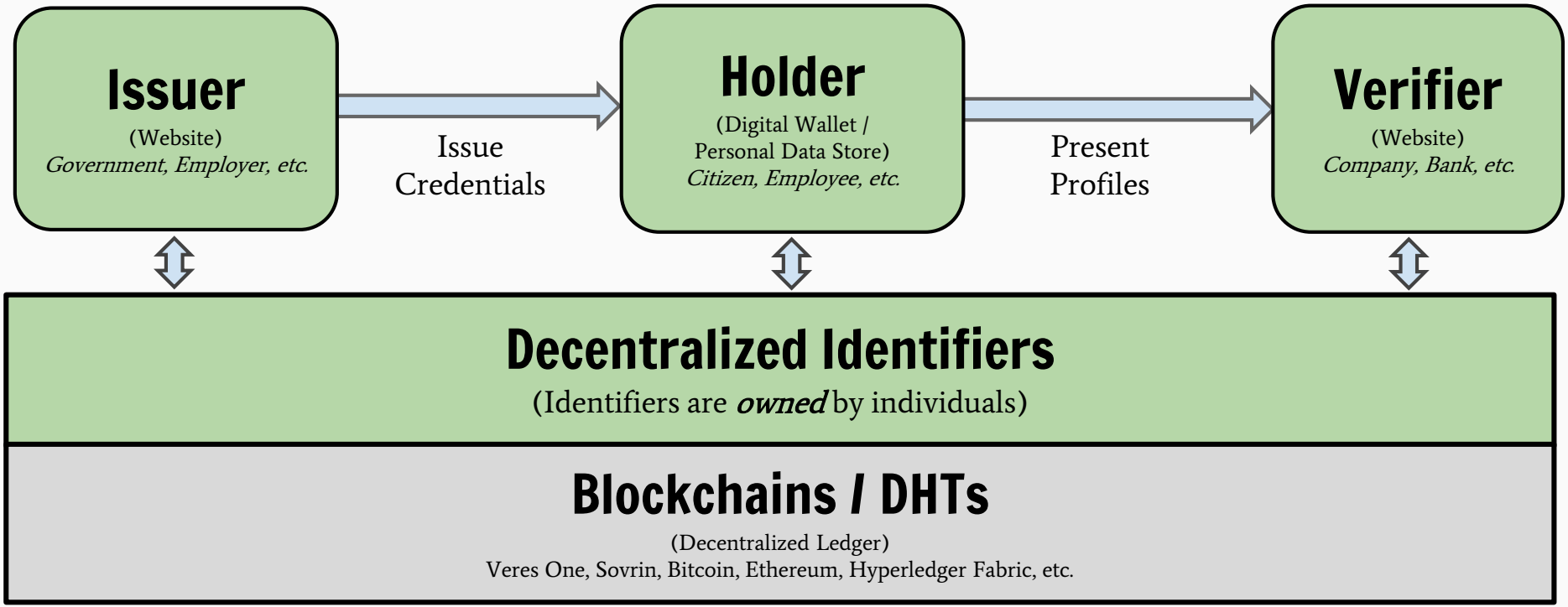
```
{
  "@context": "https://w3id.org/veres-one/v1",
  "id":
"did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
  "authentication": [{
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [{
      "id":
"did:v1:test:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD#aut
hn-key-1",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

1. Authentication Mechanisms

2. Public Key Material

3. Service Discovery

Decentralized Identifiers



W3C Community Group Draft Report

TABLE OF CONTENTS

Decentralized Identifiers (DIDs) v0.11

Data Model and Syntaxes for Decentralized Identifiers (DIDs)

Draft Community Group Report 22 January 2019

Latest editor's draft:
https://w3c-ccg.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-ccg/did-spec
File a bug
Commit history
Pull requests

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 URLs 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.