

Decentralized Identifiers and Web of Things

2020 W3C WoT VF2F



Manu Sporny | CEO | Digital Bazaar

- Co-Inventor and primary W3C spec Editor for Decentralized Identifiers, Verifiable Credentials, and JSON-LD
- Co-Founder of Veres One (DID Method)
- 10+ Years in Web Standards
- Customers in Finance, Government, Education, and Healthcare

Email: msporny@digitalbazaar.com

Twitter: [@manusporny](https://twitter.com/manusporny)

<https://www.linkedin.com/in/manusporny/>

Anatomy of a Verifiable Credential



- <IDENTIFIER>
 - license: I1234562
 - hair: BLK
 - name: ALEXANDER JOSEPH
 - address: 2570 24th STREET ...
 - date of birth: 08/31/1977
 - issued by: California DMV
 - digital signature: MIIB7ZueKqp...

Which identifiers do we use today?



jdove@bigcorp.com

555-867-5309

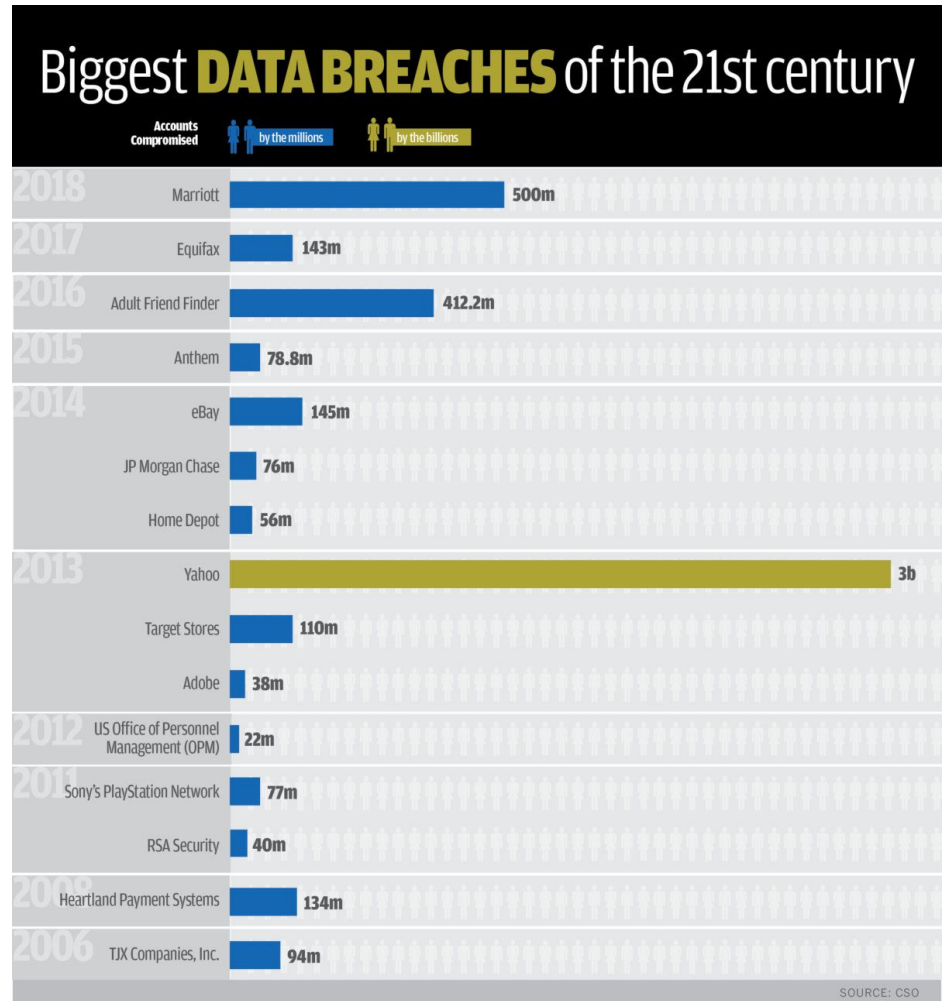
https://flitter.com/jdove

Why is this a problem?

**EQUIFAX
BREACH**

- ▶ 143 MILLION AMERICANS
- ▶ NAMES, ADDRESSES
- ▶ SOCIAL SECURITY NUMBERS

The graphic features the text 'EQUIFAX BREACH' in large, bold, red and white letters. Below it, three yellow arrows point to the text '143 MILLION AMERICANS', 'NAMES, ADDRESSES', and 'SOCIAL SECURITY NUMBERS'. The background is a blue grid with a fingerprint pattern.



What is missing?

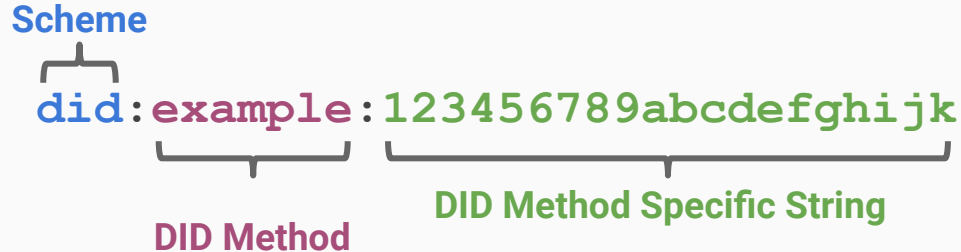
Many portable identifiers for any person, organization, or **thing** that do not depend on a centralized authority, are protected by cryptography, and enable privacy and data portability.

Decentralized Identifiers

A new type of URL that is:

- globally unique,
- highly available,
- cryptographically verifiable,
- with no required central authority.

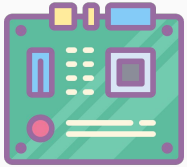
What does a DID look like?



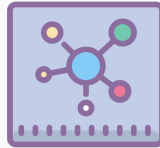
Example:

`did:v1:nym:z279u9eqhDa9CQMLYr8KRJRGcGAsTku4nQsipLDnHszaFaXV`

Web of Things and DIDs



IoT Device



IoT Gateway



WoT Service Provider



Manufacturer



Legal Controller

DIDs Resolve to DID Documents

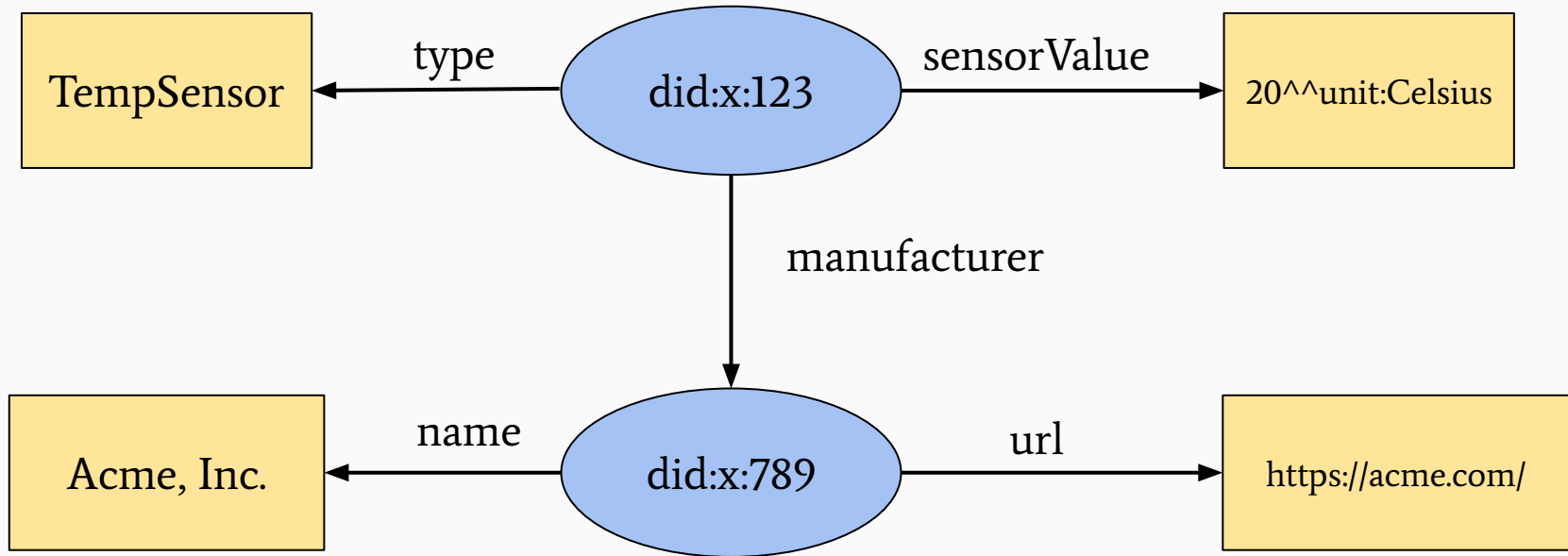
```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:key:zDwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
  "authentication": [{
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [{
      "id": "did:key:zDwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD#authn-key-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:key:zDwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
      "publicKeyBase58": "DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD"
    }]
  }],
  "service": [{
    "type": "ExampleCoAPMessagingService2020",
    "serviceEndpoint": "coap://overlay-1.example.com/proxy-1/"
  }],
  ... more DID-specific information here ...
}
```

1. Authentication Mechanisms

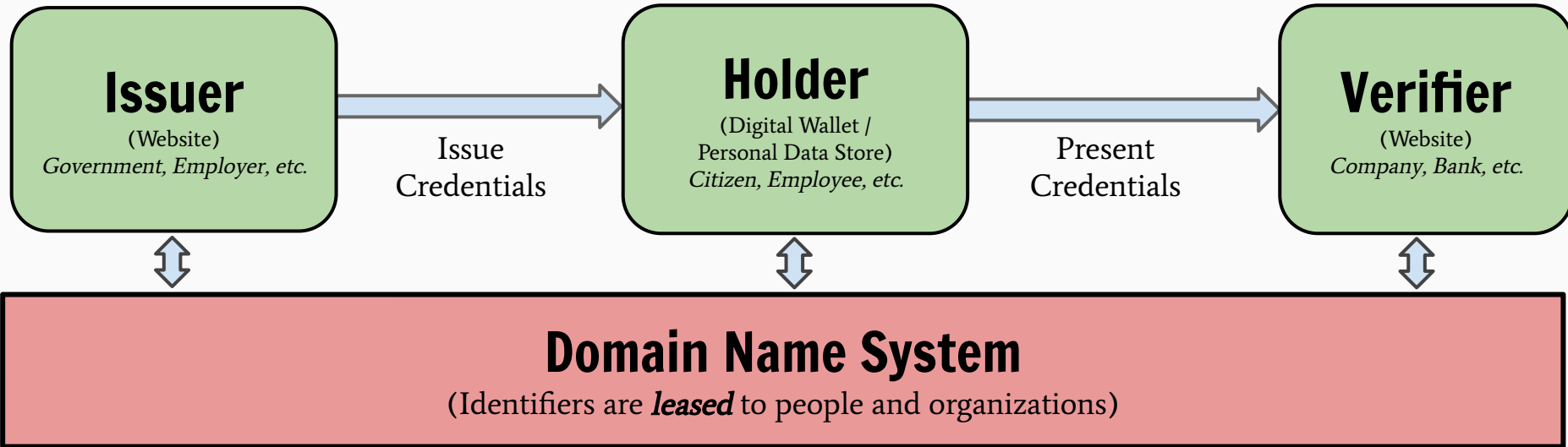
2. Public Key Material

3. Service Discovery

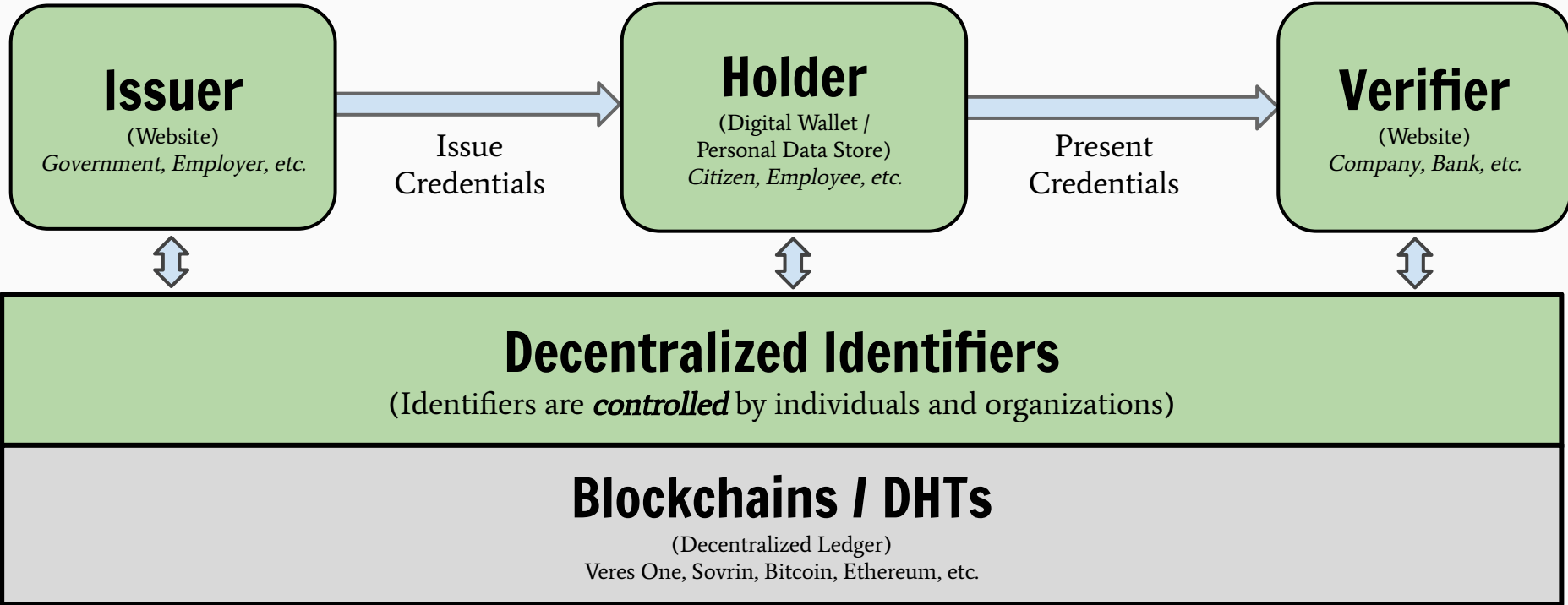
We use DIDs in Verifiable Credentials



Web Identifiers Today



Decentralized Identifiers



1. **Introduction**
 - 1.1 A Simple Example
 - 1.2 Design Goals
 - 1.3 Interoperability
2. **Terminology**
3. **Overall Architecture**
 - 3.1 DIDs
 - 3.2 DID Registries
 - 3.3 DID Documents
 - 3.4 DID Resolvers and DID Resolution
 - 3.5 Security and Privacy
4. **Conformance**
5. **Identifier**
 - 5.1 DID Syntax
 - 5.1.1 Generic DID Syntax
 - 5.1.2 Method-Specific Syntax
 - 5.1.3 Normalization
 - 5.1.4 Persistence
 - 5.2 DID URL Syntax
 - 5.2.1 Generic DID URL Syntax
 - 5.2.2 Generic DID URL Parameters
 - 5.2.3 Method-Specific DID URL Parameters
 - 5.2.4 Path
 - 5.2.5 Query
 - 5.2.6 Fragment
6. **Data Model**
 - 6.1 Definition
 - 6.2 Extensibility
 - 6.3 Representation Requirements
7. **Core Properties**

Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations



W3C Working Draft 12 March 2020

This version:

<https://www.w3.org/TR/2020/WD-did-core-20200312/>

Latest published version:

<https://www.w3.org/TR/did-core/>

Latest editor's draft:

<https://w3c.github.io/did-core/>

Previous version:

<https://www.w3.org/TR/2019/WD-did-core-20191209/>

Editors:

[Drummond Reed \(Evernym\)](#)

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

[Markus Sabadello \(Danube Tech\)](#)

Authors:

[Drummond Reed \(Evernym\)](#)

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

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

[Christopher Allen \(Blockchain Commons\)](#)

[Ryan Grant](#)

[Markus Sabadello \(Danube Tech\)](#)

Participate:

[GitHub w3c/did-core](#)

[File a bug](#)

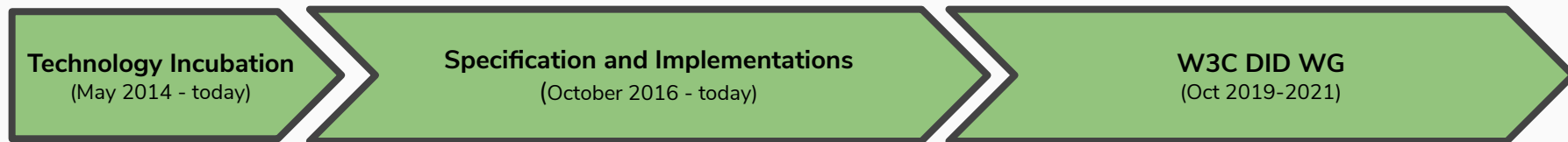
[Commit history](#)

[Pull requests](#)

Copyright © 2020 W3C[®] (MIT, ERCIM, Keio, Beihang). W3C liability, trademark and permissive document license rules apply.

Decentralized Identifiers Status

Roadmap



Weekly Community Group Participants: **15-28 / 345**

Spec/Issue Regular Contributors: **32**

Known Implementing Companies: **51!!!**

[Join the DID WG](#)

Other WoT - DID Related Specs

- [Verifiable Credentials](#)
 - Enables WoT devices to assert cryptographically verifiable statements.
- [Encrypted Data Vaults](#)
 - Protected data in transit and at rest.
- [Linked Data Proofs](#)
 - Cryptographically sign/protect JSON-LD data using DIDs.
- [Authorization Capabilities](#) (ZCAPs)
 - Cryptographic authorization and delegation to protected services.
- [HTTP Message Signatures](#)
 - Perform simple cryptographic authentication over HTTP.