Credentials Community Group Intro

Heather Vescent, CCG Co-Chair

March 2021

CCG WG: https://www.w3.org/community/credentials/
DID WG: https://www.w3.org/2019/did-wg/

Agenda

- CCG Intro, Heather Vescent
- CCG History, Manu Sporny
- DID Core, Brent Zundel
- Universal Wallet, Mike Prorock & Orie Steele
- Encrypted Data Vaults, Mike Prorock & Orie Steele
- CCG/Solid collab, Dmitri Zagidulin
- Q&A

Presenting from Joshua Tree, California

Terms

- W3C = World Wide Web Consortium
- VC = Verifiable Credential
- DID = Decentralized Identifier
- CCG = Credentials Community Group
- IPR = Intellectual Property Rights
- SVIP = Silicon Valley Innovation Program (at DHS)
- DHS = Department of Homeland Security
- DIF = Decentralized Identity Foundation
- DIACC = Digital Identity & Authentication Council of Canada
- ToIP = Trust over IP (Linux Foundation Group)
- APAC = Asia Pacific

Activities at the W3C

Community Group

- Free, open to anyone
- Some IPR processes
- Volunteer run
- Standards potential

CCG
(Credentials Community Group)

Working Group

- W3C member only
- IPR processes & infrastructure
- Formal W3C support
- Standards track

DID WG
(Decentralized Identifier Working Group)

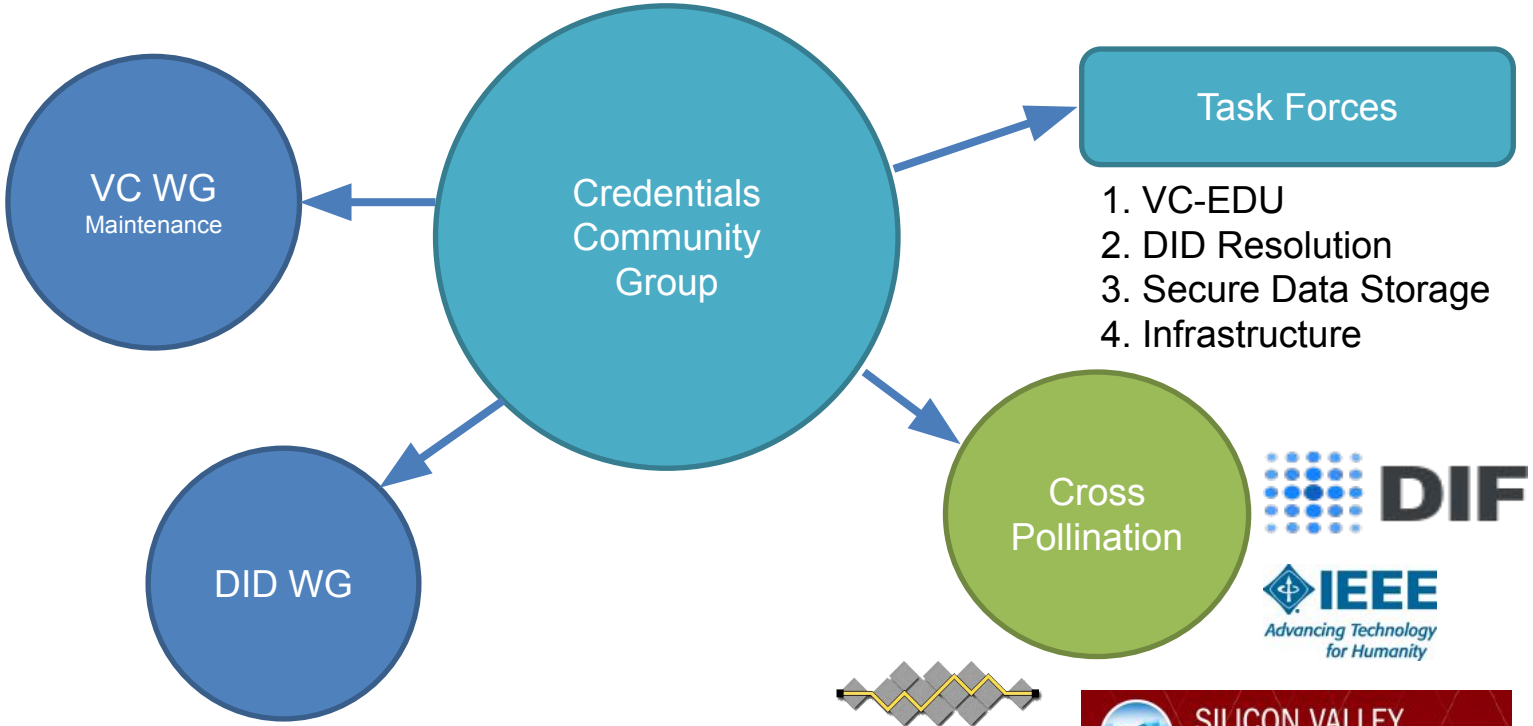
VC WG
(Verifiable Credentials Working Group)

Mission

> Explore the creation, storage, presentation, verification, and user control of credentials.

- Draft and incubate Internet specifications for further standardization and prototyping and testing reference implementations
- Seek solutions inclusive of approaches such as:
  - self-sovereign identity
  - presentation of proofs by the bearer
  - data minimization
  - centralized, federated, and decentralized registry and identity systems

CCG Community Group



Active Membership

- Open membership, not required to be W3C member
- 422 members
- 4 task forces
  - One combined with DIF
- Industries/Organizations include:
  - Education, Supply chain, Publishing, Security, Identity, Government, Technology, Cryptocurrency & Blockchain, Storage, Standards
- Active mailing list discussions
- Avg weekly attendance 25-40, sometimes 50+ for popular sessions
- https://www.w3.org/community/credentials/

Why I participate

“3Cs -- Context, candidness, and community.”

“Get a broad view of the ecosystem”

“To move beyond VC and DID to stuff people might actually understand and care about.”

“I learn stuff.”

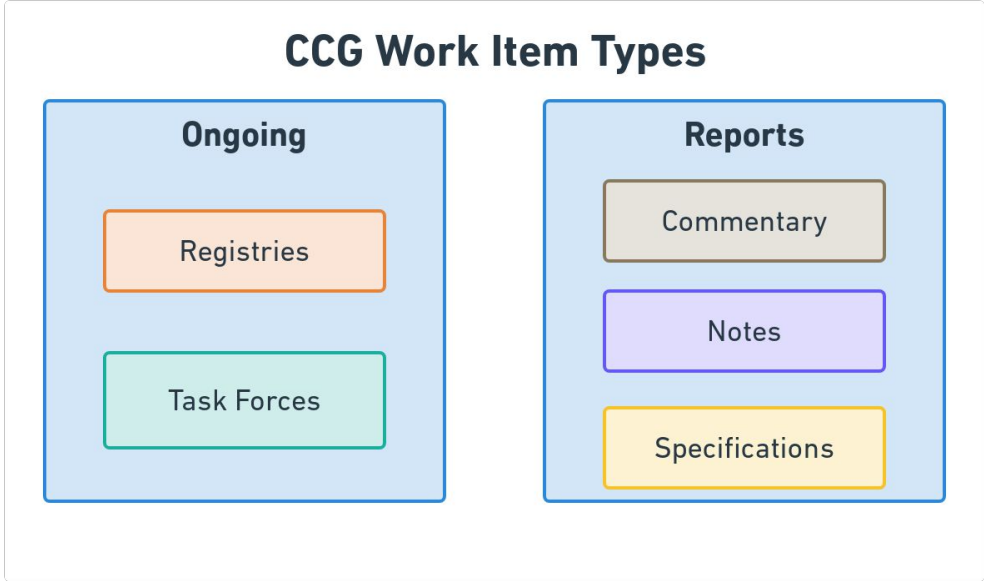
CCG Leadership

- Current Co-chair open
  - Previously held by Kim Hamilton Duffy
- Heather Vescent
  - 2 year seat (ends Summer 2022)
  - Operations, strategy, inclusion, APAC, outreach & evangelism
  - (Can we reduce unintended consequences of future technology?)
- Wayne Chang
  - 3 year seat (ends Summer 2023)
  - Technical operations, APAC, wallets

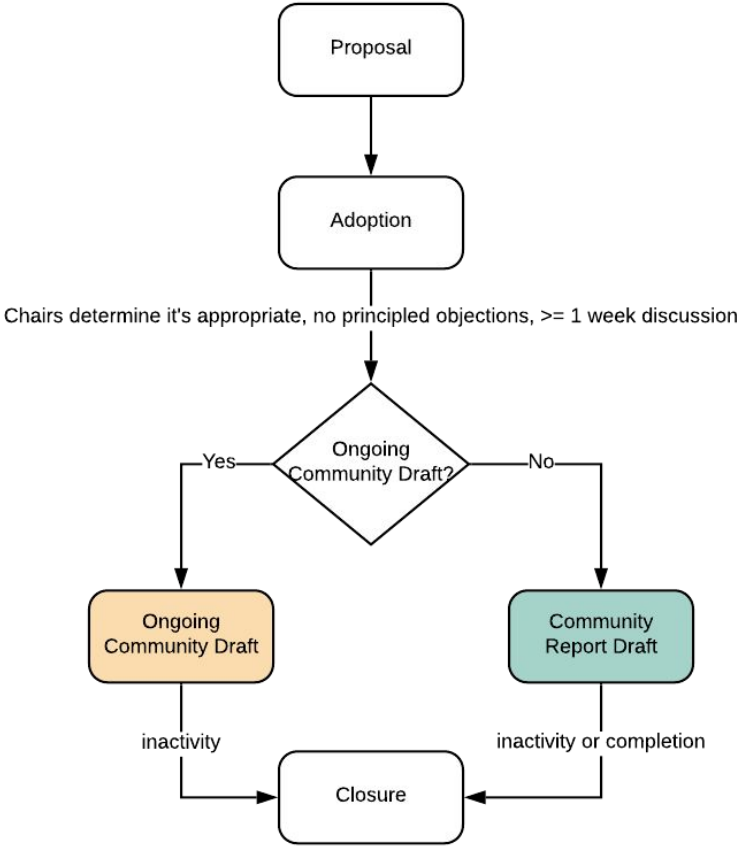
The Task Forces

- Verifiable Credentials for Education
  - Explore what's needed to enable educational ecosystem use of VCs
  - Developing guidance for use of VCs with EDU data standards (internationally)
  - Deliver guidelines, best practices, and prototypes
- DID Resolution
  - Complements DID WG
  - How to achieve DID resolution interoperability across DID methods
- Secure Data Storage (co-hosted with DIF)
  - Unified separate standardization efforts (Identity Hubs, Encrypted Data Vaults and more)
  - Jointly run by DIF and CCG (thank you to W3C staff!)
- Infrastructure Task Force

Work Items



Work Item Process Overview



W3C Credentials CG History

VCs 1.0 and DIDs

2014-2017

- Web Payments: Shipping preferences, loyalty cards, strong authentication
- Education: Low-stakes and high-stakes credentials

DIDs and LD Crypto

2017-2019

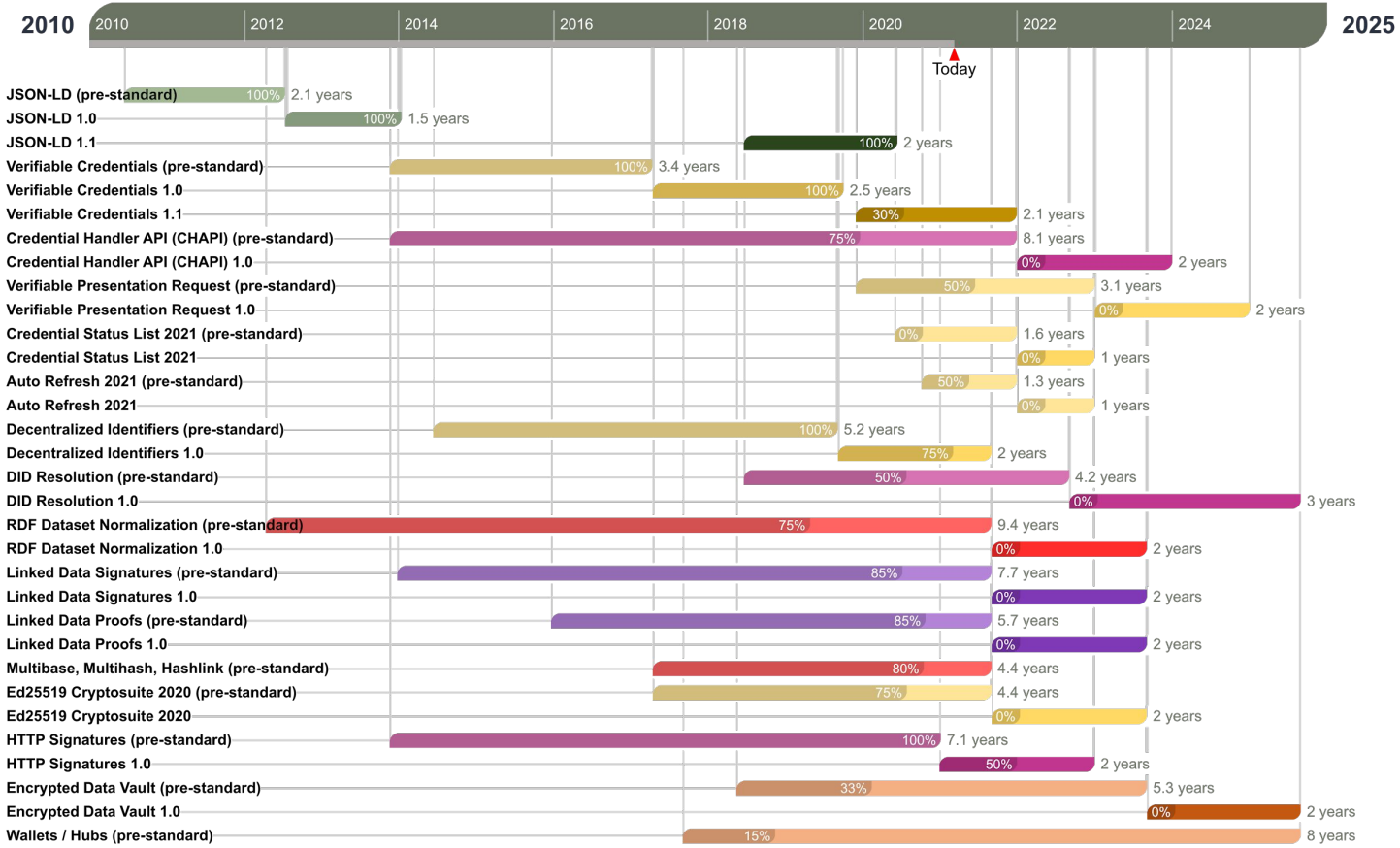
- Strong authentication and VCs for Supply Chain and Non-person Entity use cases
- Blockchain-based cryptographic proof mechanisms (proof of work, stake, spend, etc.)

VCs 2.0 and Storage

2019-Present

- Strong authentication and VCs for privacy-preserving student, citizen, employee use cases
- Wallet protocols, data portability, encrypted storage, and data privacy

Solid / CCG Work Item Overlap



DID Core (Brent)

Decentralized Identifiers (DIDs)

A globally unique identifier (URI) that does not require a centralized registration authority because **control of the identifier can be proved using cryptography**.

evernym

Why DIDs?

DIDs were originally born out of a need in Verifiable Credentials for an identifier that couldn't be taken away.

If a credential is issued to someone, whether they can continue using the credential shouldn't depend on an entity beyond the Issuer or the Holder.

DIDs have four core properties:

1. User-controlled

You can keep it as long as you need it

2. Resolvable

You can look it up to discover metadata

3. Cryptographically-verifiable

You can prove control using cryptography

4. Decentralized

No centralized registration authority is required

evernym

Comparison of DIDs with URLs and email addresses

Property	URL	Email	DID
User-controlled	✘	✘	✔
Resolvable	✔	✘	✔
Cryptographically-verifiable	✘	✘	✔
Decentralized	✘	✘	✔
Human-friendly	✔	✔	✘
Trust Model Flexibility	✔	✘	✔

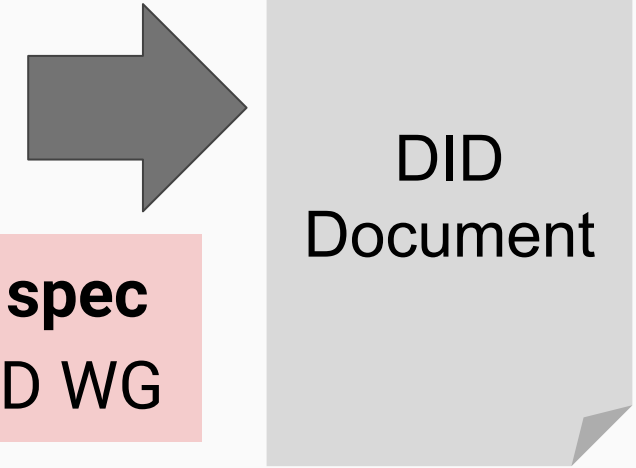
DID Design

- The DID spec does not define an identity system
  - DIDs are designed to be part of identity systems
- DID is a stable identifier, bound to a set of public keys.
- **DID Methods** enable different trust models, e.g.:
  - **did:peer** - peer-to-peer communication of key changes
  - **did:ion** - keys are backed by crypto-blockchains
  - **did:sov** - non-profit governance of a distributed ledger
  - **did:web** - relies on DNS

DID Resolution...

Is the process of using the DID to get a copy of the DID Document as defined by the DID Method

did:sov:21tDAKCERh95uGgKbJNHYp



Note: DID Resolution is a **separate spec** that is out-of-scope for the W3C DID WG

A DID Document...

Contains metadata for describing and interacting with the DID Controller

1. **Public keys** or other cryptographic proof material
2. **Service endpoints** for engaging in trusted interactions
3. **Authentication options** for proving control of the DID
4. **Other metadata** helpful in discovery & verification

DIDComm

https://github.com/decentralized-identity/didcomm-messaging

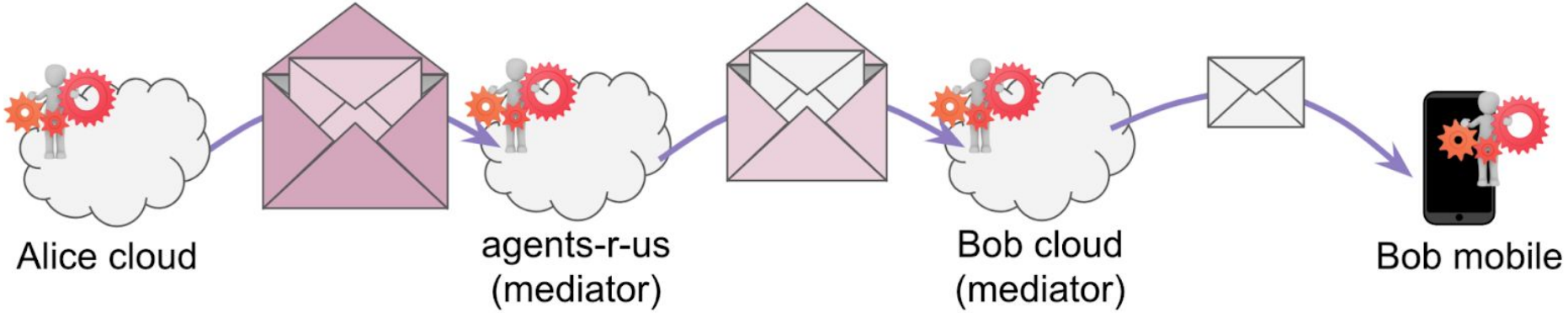
- Use DIDs for secure communication
  - V1 has been in production since late 2018;
  - V2 under development at DIF (Decentralized Identity Foundation)
- Can be used with
  - Any DID method
  - Any transport: HTTP, file system, email, BlueTooth, CHAPI, AMQP, Kafka, etc
  - Peer-to-peer: use your DID for authenticated pairwise or n-wise encr
  - Broadcast: use your DID to sign a message to the world (QR, mailers, etc)
  - Web: client/server with RESTful or similar
- Uses JOSE stack (JWM, JWS, JWE)

How DIDComm Works

service endpoints

routing

authenticated encryption



DIDs and Authentication

DIDs may address some challenges in Authentication systems

- Public-key distribution
  - DIDs can be resolved into DID Documents, which contain up-to-date public-keys and communication endpoints.
- Single identifier, multiple keys
  - DID Documents may contain multiple public keys, all tied to a single identifier

Status of DID 1.0 specification

- Incubated in W3C Credentials Community Group
- W3C DID Working Group started in September 2019
- Expecting DID 1.0 => Candidate Recommendation by next week.
- DID spec is a data model.
    - We define the DID Resolution interface, but the resolution process itself is out of scope.

Universal Wallet (Orie & Mike)

- https://w3c-ccg.github.io/universal-wallet-interop-spec/storybook/?path=/story/plugins-did-key--did-key

Encrypted Data Vaults (Orie & Mike)

- https://github.com/decentralized-identity/confidential-storage

Collaborate

- Credentials Community Group
  - Meetings: Tuesday, 9am Pacific / Wednesday, 1am Korea (KST)
  - Join: https://www.w3.org/community/credentials/
  - Website: https://w3c-ccg.github.io/
  - Mailing list: public-credentials@w3.org
  - Github: https://github.com/w3c-ccg
- DID WG
  - Meetings: Tuesday, 8am Pacific / Wednesday, Midnight Korea (KST)
  - Website: https://www.w3.org/2019/did-wg/
  - DID Primer: https://w3c-ccg.github.io/did-primer/
- VC WG: https://www.w3.org/groups/wg/vc

Collaboration comments (Dmitri)

See several areas for collaboration

- DIDs: https://github.com/solid/specification/issues/217
- Confidential Storage
- Identity Hubs

Thank you & Questions

Credentials Community Group

Next steps?

- Join calls
- present the use case to the confidential storage call
- tour of the spec, how does it work, how can we try it out, get hands dirty,