

## Application Layer (Use Case)

### Legend

- Stable, Externally-known
- Stable
- Experimental or In-Progress
- \*\* = [better] citation needed! Comments or github issues welcome

## Credential Layer (Verifiable Data)

### Sample Apps

TrustPing

### Semantic Data Def

ActivityPub  
schema.org  
Open Badges  
Learner Record  
FHIR

### Verticals

Education  
Work Certificates  
Social  
Health

## Vertical / Cross-Cutting

### AuthN/AuthZ

WebAuthn (FIDO2)  
2.0  
SIOP  
0.3  
...

### Cred Format

OpenID Connect id\_token  
Open Badges  
Verifiable Credential  
Verifiable Presentation

### Cred Proof

VC JSON-LD Proofs  
VC-JWT  
AnonCreds v1  
AnonCreds v2 \*\*  
whitepaper

### Cred Revocation

XSD9 DCSP/CRL \*\*  
VC Status Revocation List  
AnonCreds v1  
AnonCreds v2 \*\*  
ESSIF \*\*

### Cred Exchange

Aries Present Proof v2  
Presentation Exchange  
VP Request (CCD)  
Credential Manifest  
OIDC Credential Provider

### Cred Binding

DID  
OpenID Connect id\_token  
Link Secrets (CL-RSA / idemix)

### Disclosure/ZKP

Anoncreds v1 ZKPs  
BBS+ signatures  
Snark-Credentials

### Compliance

eIDAS  
CCPA  
EFF  
FISMA  
GDPR

P2P-Communication

Proof / Signature Generation

Proof / Signature Verification

Key Access

Storage

### Envelope

JWM (IETF draft)  
DID Comm v1  
Self-Issued OpenID Connect Provider DID Profile v0.1  
DID Comm v2 (JWM)

### Transport

NFC  
BLE  
QR  
HTTP  
CHAPI

### Control Recovery

Trezor BIP-39  
Mortcrux Protocol  
SeedQuest  
Fuzzy Vault  
Universal Wallet CCG  
DKMS  
Shamir-secret recovery mechanisms

### Key Operations

"Cloud" HSM  
On-Prem/Local HSM (Hardware Security Module)  
TEE chips  
NFC "Smart Cards," etc.

### [Meta]Data Portability

Universal Wallet CCG

### Storage

"centralized" storage (MySQL, CouchDB, MongoDB)  
IPFS  
On-Chain (Proprietary)  
Web Server (Proprietary)  
Solid  
Ceramic  
Secure Data Store (SDS) = EDV v2 + Identity Hub v2  
Semantic Containers

### Data Formats

NOT AN EXHAUSTIVE LIST  
JSON \*\*  
XML \*\*  
ASN.1 \*\*  
CBOR \*\*

## Agent Layer (Communication, Storage, Key Management)

DID-Document Verification

DID-Document CRUD Interface

DID Document State

Storage

### DID Document

DID CCG 1.0  
DID Core WG editors draft  
DID Document ESSIF \*\*

### DID Methods/Ops \*

NOT AN EXHAUSTIVE LIST  
did:element  
did:ethr  
did:key  
did:github  
did:gitcoin  
did:ion  
did:sov  
did:v1  
did:work

### DID [Doc] History

Revocable/Null DIDs \*\*  
Current-only State \*\*  
Queryable Historic States \*\*

### DID Resolution

uniresolver.io  
DID Resolution  
DID Dereferencing  
Peer DIDs

### DID-Anchored Svcs

Identity Hubs  
EDV (Encrypted Data Vault)  
Messaging Endpoint  
Secure Data Store (SDS) = EDV v2 + Identity Hub v2

### Timestamping

Proprietary  
Open Timestamps

### Crypto Primitives

NOT AN EXHAUSTIVE LIST  
RS256  
ES256 \*\*  
secp256k1

## Public Trust Layer (Anchor)

### DID Scaling

Sidetree Editor's Draft  
Sidetree v1.0  
KERI

### Anchor Types

Non-DLT consensus ledger (i.e. KERI)  
Veres One \*\*  
Sovrin Network \*\*  
Bitcoin Mainnet \*\*  
Ethereum \*\*

The Interoperability working group at the DIF has been doing outreach, interchange, and ideation work to get the ball rolling and make clear the diversity of solutions and architectures already developing in the decentralized identity space. This map was one of the first major programs, expanding on the [earlier work](#) of DIF Executive Direction Rouven Heck at #IIW30, which was in turn indebted to the high-level Aries 4-layer [mapping](#). The map quickly grew less tidy, with the addition of a transversal category and protocols *between* layers.

Each column on our “map” of options available to architects of decentralized identity solutions represents the “implementation choices” which an architect or CTO designing a decentralized identity system or component would need to make. These can be understood as follows:

### ***Credential Layer (aka “Verifiable Data”):***

How Verifiable Credentials are handled, exchanged, and verified. This layer *may* interact with VC-handling systems that do not use DIDs, and thus look very different on lower layers!

- **Credential Formats:** which kinds of credentials can you receive, issue, verify, etc?
- **Credential Proofs:** how VPs are signed.
- **Credential Revocation:** how is the status of VCs revoked and/or checked?
- **Credential Exchange:** what protocols or assumptions determine how credentials are exchanged between parties?
- **Credential Binding:** What identifier is written into VCs as the subject?

### ***Agent Layer (aka “Mechanics”):***

"Cloud Agents," microservices, APIs and backends live on this layer. It includes communication services, data storage (including storage of VCs), and Key Management.

- **Agent-to-Agent Envelopes:** To secure communications, you need to sign packets, but many different mechanisms and philosophies apply.
- **Transport:** However data and messages get enveloped, those envelopes need to travel!
- **Control Recovery:** However control is proven or exerted, it needs to be recoverable after loss or systems failure.
- **Key Operations:** BYO keys and enterprise key management are hard to integrate with SSL.
- **[Meta] Data Portability:** Is a wallet a lifetime commitment, or can they be migrated between?

### ***Public Trust Layer (aka “Anchoring”):***

DIDs, blockchains/DLTs, and other mechanisms for establishing trust between and across decentralized identity systems live on this layer.

- **DID Methods & Anchor Types** vary widely!
- **DID Document:** Which version does your DID Docs conform to, and are you ready for everyone else’s?
- **DID Doc History:** Do you keep (or query) old docs?
- **DID Scaling:** Scaling up DIDs beyond DLT constraints
- **DID Resolution:** How to get Docs for others’ DIDs
- **DID-Anchored Svcs:** These communication and storage services are fully encrypted to specific DIDs

### ***Transversal Layer (aka “Cross-Cutting”):***

These are technology choices with consequences across multiple layers.

- **Authorization & Authentication:** How access or permissions get passed around between layers, between actors, and between systems.
- **Selective Disclosure (aka ZKP, Zero-Knowledge Proofs):** Showing a subset of the contents of a verifiable credential without compromising anonymity, correlation resistance, or anonymity.
- **Compliance:** Making data legal to use in specific contexts or regions requires some top-down work.
- **Storage:** There are many options for storing VCs and other identity-related data and metadata, incl. immutable, replicating, and expressive options.
- **Data formats:** Which low-level encoding is “native” to your system, and which need translators?
- **Ordering:** What is timestamped, and how tightly?