Avast

A brief introduction to decentralized identity

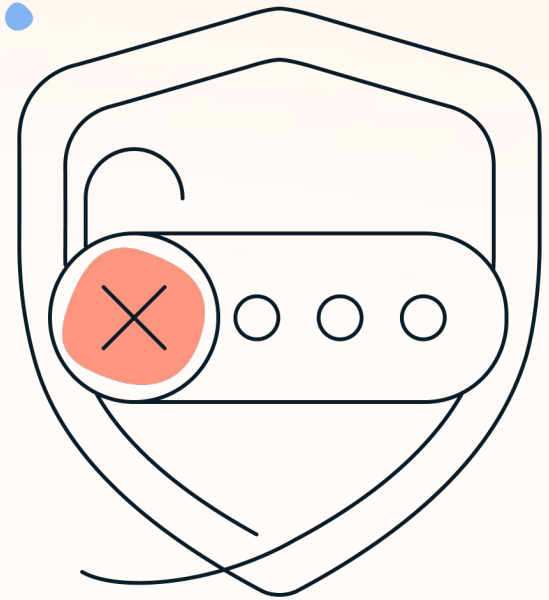
And the standards and protocols that make it possible

07 June 2022
Drummond Reed
Director, Trust Services

The problems today

The Internet is missing a “trust layer”

- We have no control over our data
  - Instead, we entrust it to third-party servers and databases, subject to breaches and data misuse.
- We don’t have a way to take our identity data with us
  - With no data portability or reusability, we’re forced to create a new account with every website or service we want to use – endless forms and hundreds of user accounts
- We have no easy way to verify information about ourselves or others
  - Claims are either self-attested or verified using costly, admin-heavy methods



Hardly a day goes by without headlines like these

We already have a solution to this

...in the physical world

Paper or plastic credentials that are:

- Issued from a trusted source
- Tamper-resistant
- Secure
- Private
- Portable
- Reusable
- Standardized

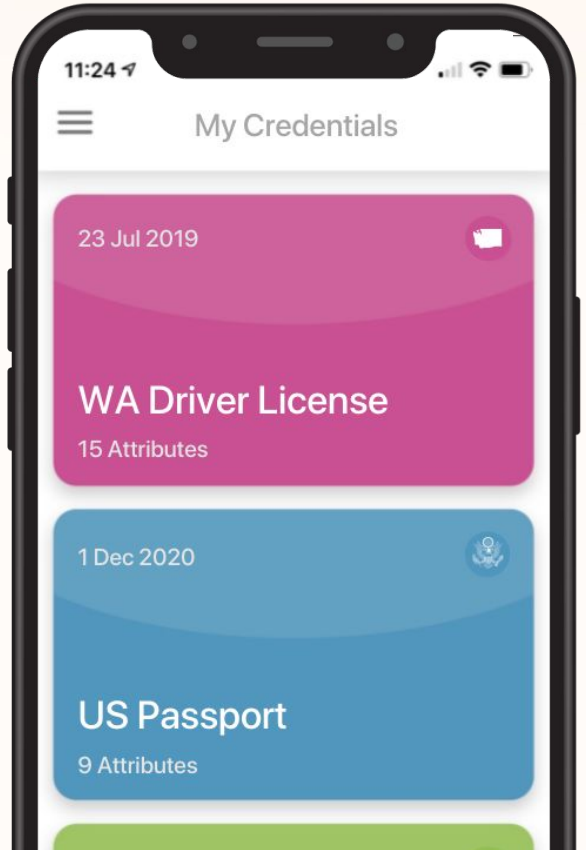
You hold the data (credential) and can show it to anyone, anywhere – on your terms.

Decentralized identity takes this same approach and makes it digital

Like your physical passport or license, verifiable digital credentials are under your control, stored on your phone, and can be shown to anyone, anywhere.

Once shared, they can be immediately verified by the receiving party, who can check:

1. Who issued the credential?
2. To whom was it issued?
3. Has it been tampered with?
4. Has it been revoked?



It puts you in the center of your digital world

centralized/federated

decentralized

And it’s gaining momentum around the world

Bonifii (US)

Trusted authentication and secure messaging for credit unions

FCA (UK)

Smarter KYC/AML for banks and fintechs

IATA (Global)

Verifiable health and travel records for global travel

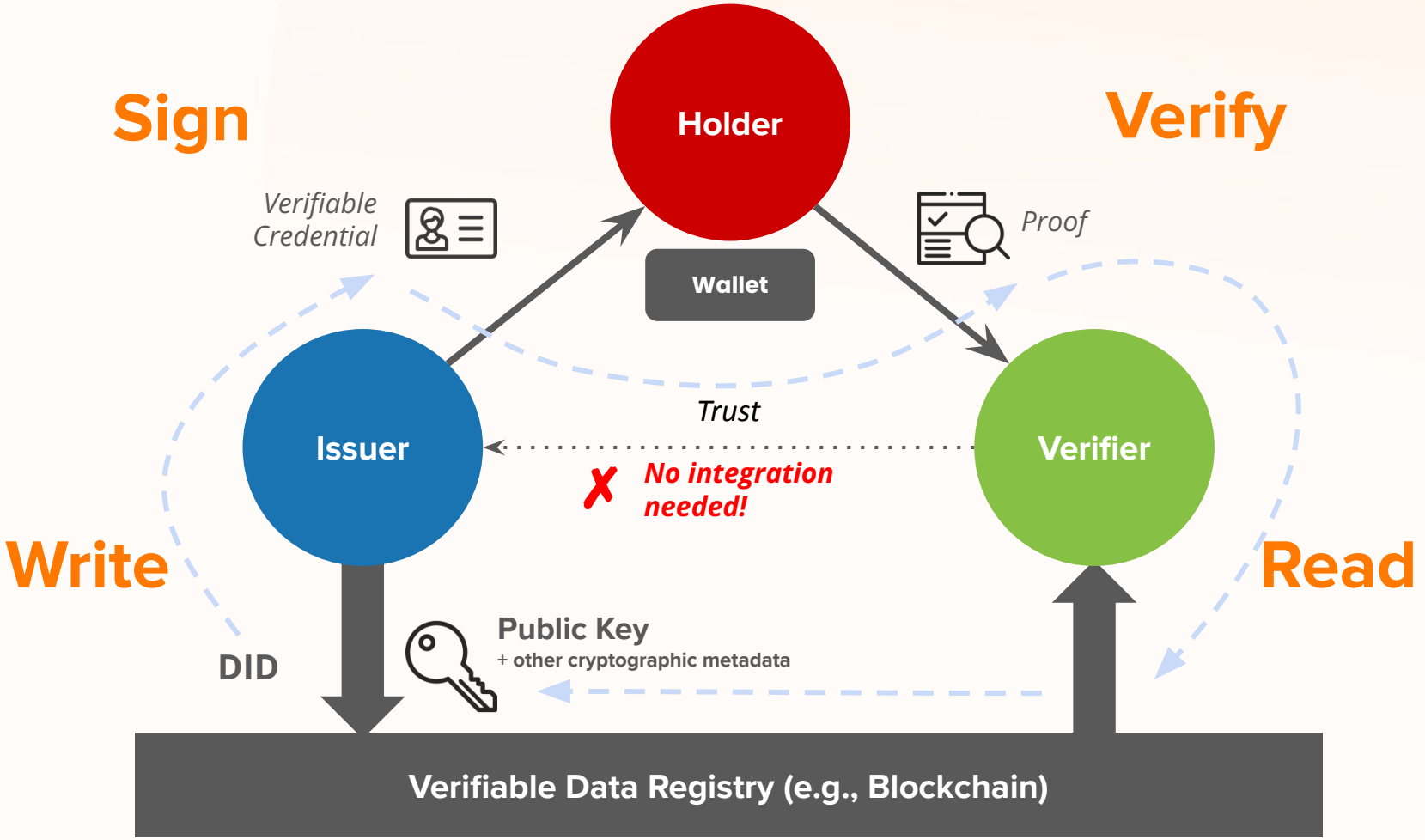
NHS (UK)

Staff ‘passports’ for streamlined access control

EU Digital Wallet

Reusable identity for all Europeans

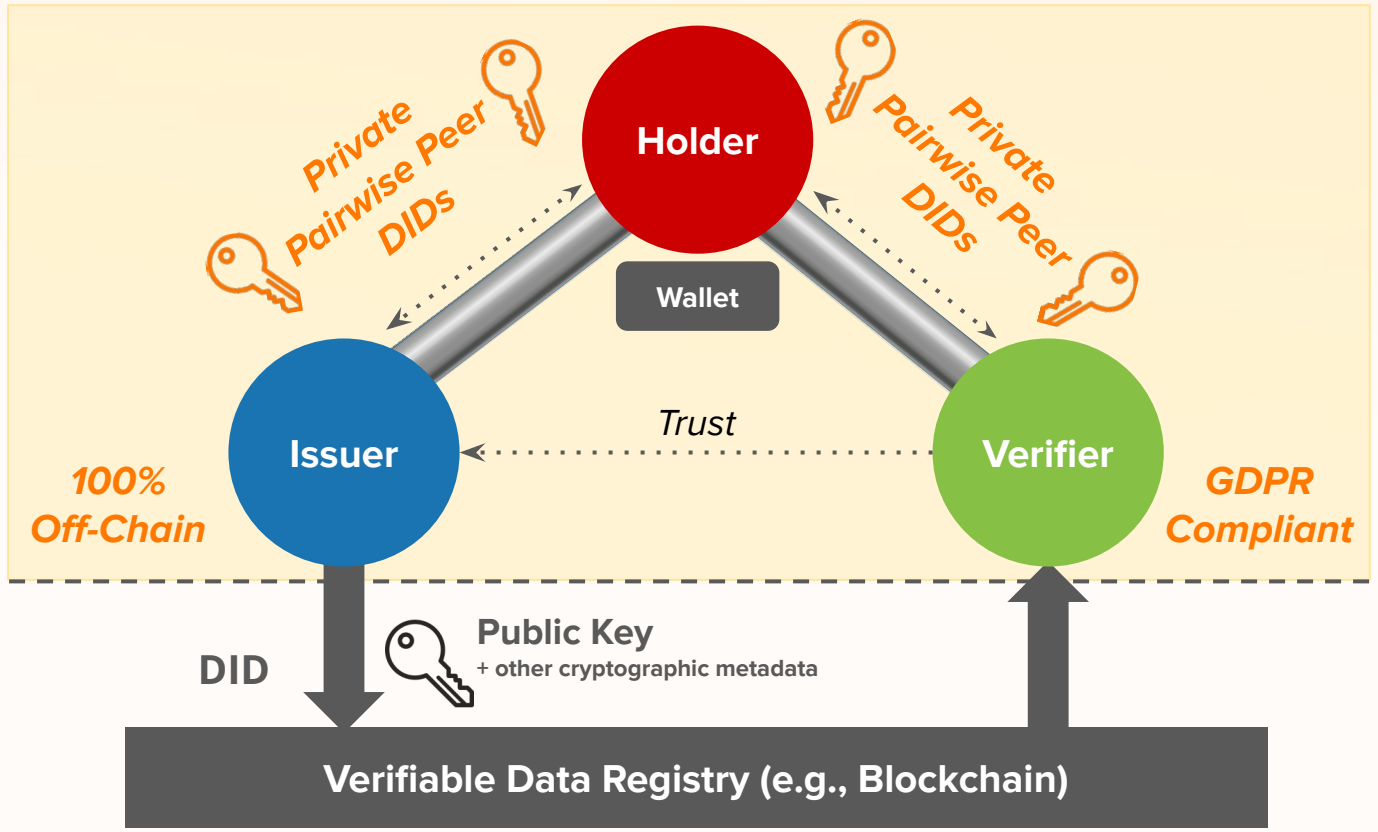
It’s all based on the “trust triangle”



Privacy by Design

At Internet Scale

- **All communication channels are private and encrypted**, using pairwise peer DIDs
- **All data is stored off-chain**, securely inside of the user's digital wallet
- **Fully GDPR compliant**, with consent-based data sharing and data minimization through zero-knowledge proofs



Benefit 1: An end to data overcollection

Individuals control what credential data they show and to whom they show it

Age verification **without** privacy protocols and zero-knowledge proofs:

- Date of birth
- First Name
- Last Name
- Photo
- Address
- Height
- Weight
- Eye color
- Sex
- License Number
- License Class
- Issue Date
- Expiration Date
- Donor Status

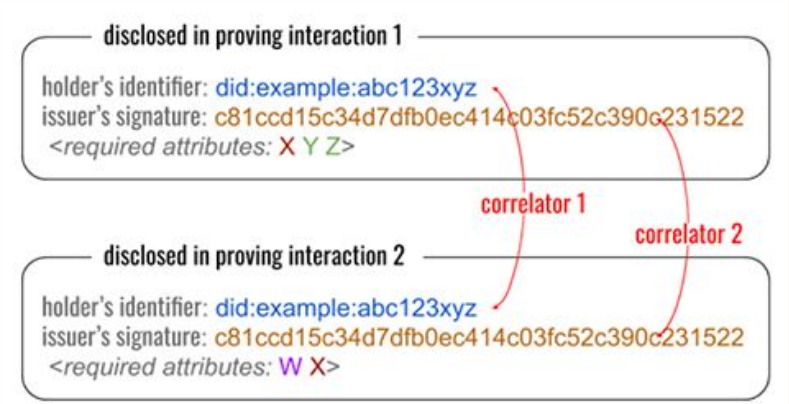
Age verification **with** privacy protocols and zero-knowledge proofs:

- Holder is over 21

Benefit 2: And end to tracking / correlation

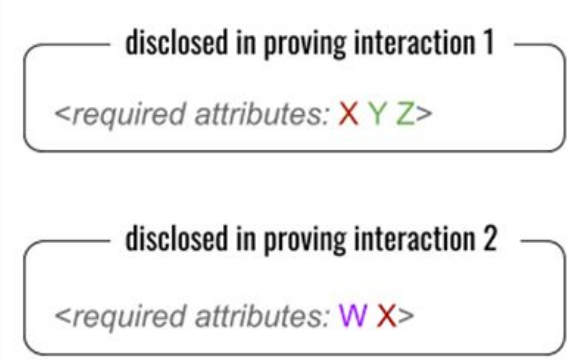
Your data and communications are always safe and private

Digital signatures
without privacy protocols
and zero-knowledge proofs:



An issuer's digital signature is the **same** for every use of a credential, creating a 'super-cookie' correlating all of your behavior.

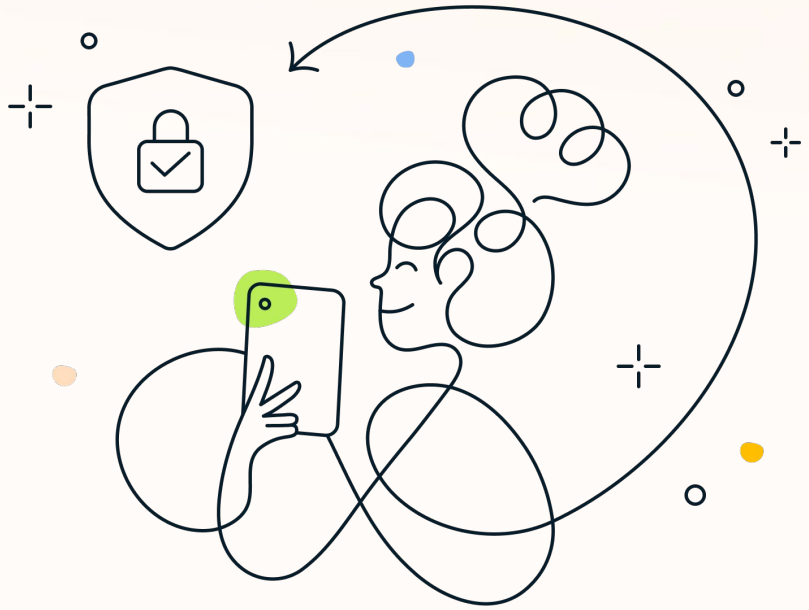
Digital signatures
with privacy protocols
and zero-knowledge proofs:



Each signature is **unique**, greatly reducing the risk of correlation and tracking.

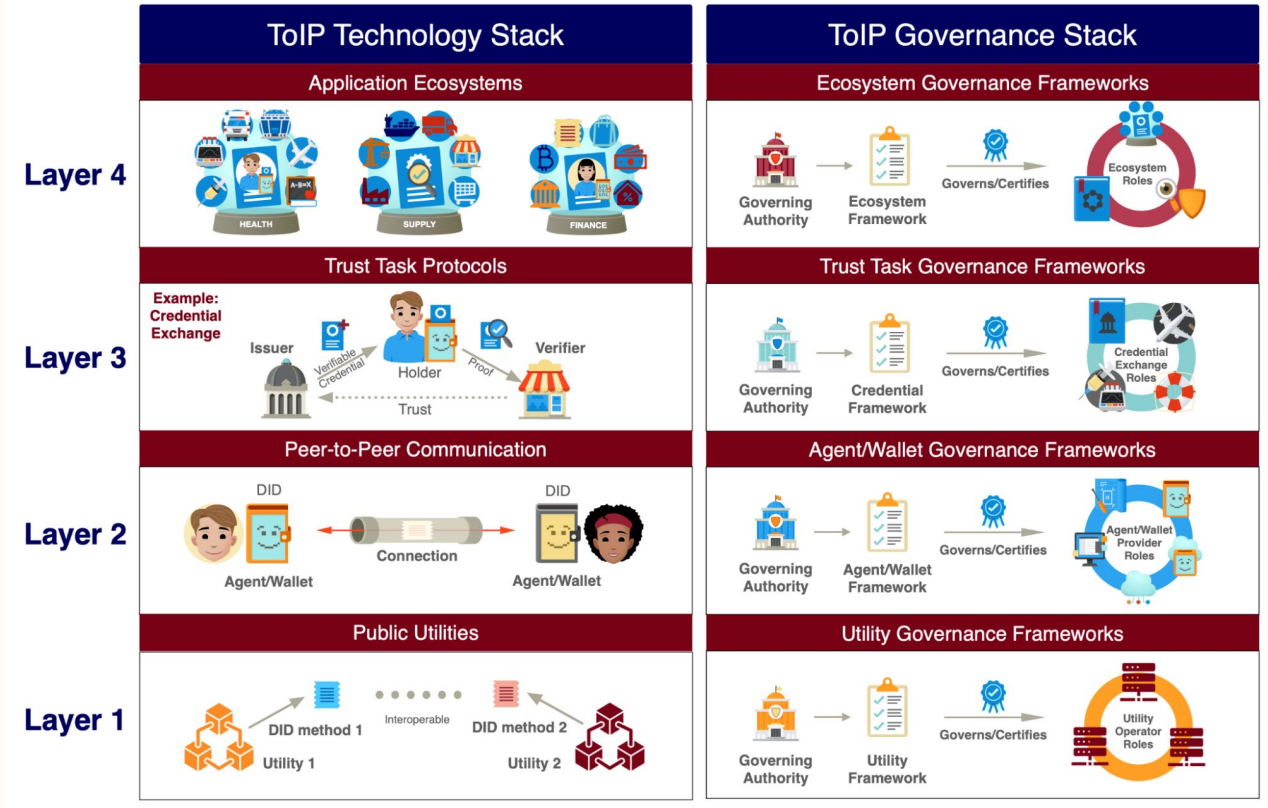
It’s made possible by open standards that the Avast team helped create

- **W3C Verifiable Credential (VC) Spec**
  - Approved as an official web standard in 2019
- **W3C Decentralized Identifier (DID) Spec**
  - Pending a vote to become an official web standard
- **DIF DIDComm V2 Spec**
  - Nearing completion in DIF DIDComm WG
  - Next step is formal standardization at IETF and/or ISO

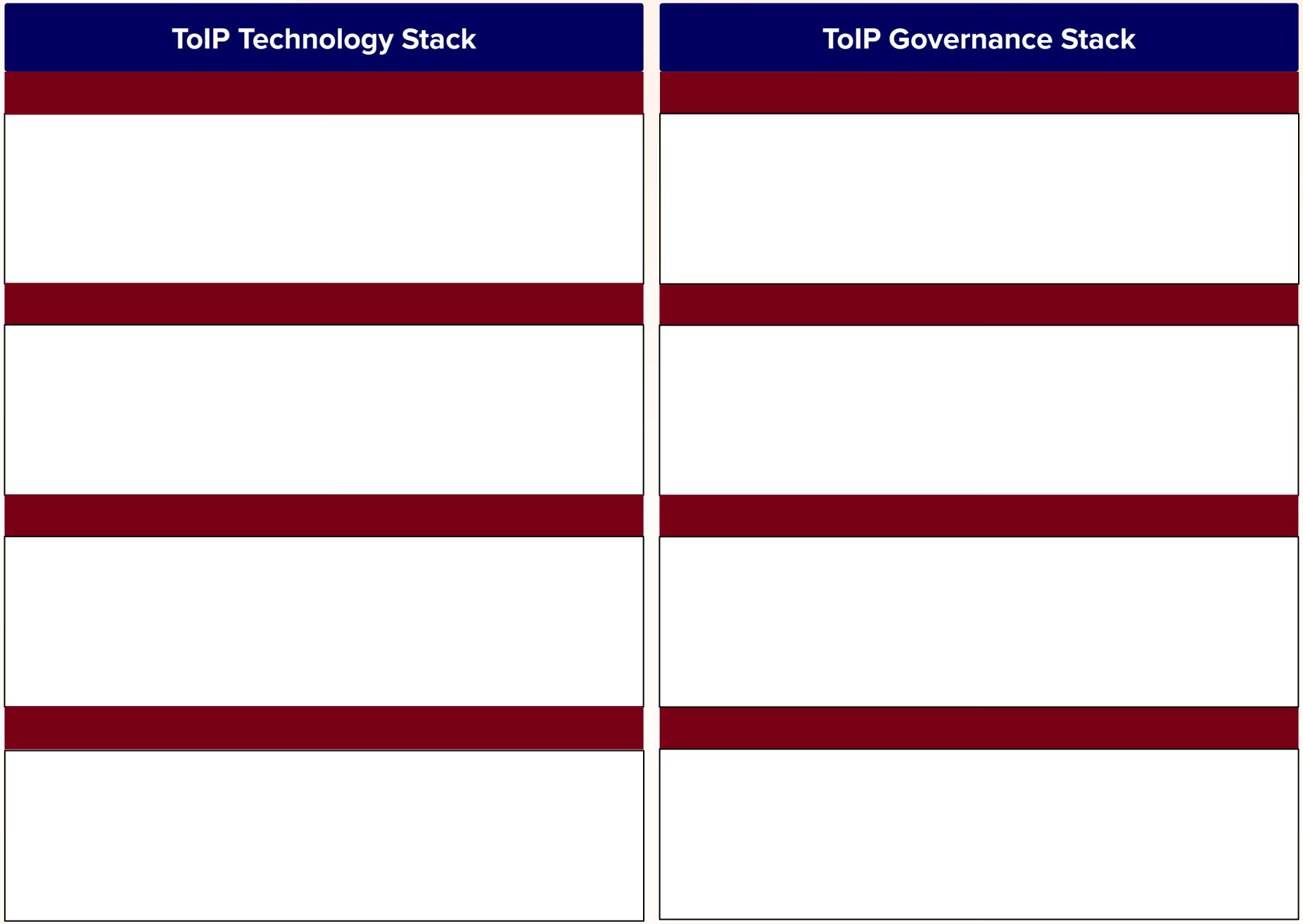


But it's about more than the technology

Governance and trust frameworks are critical



TRUST Over IP FOUNDATION

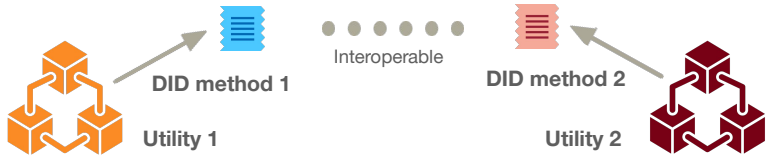

ToIP Technology Stack
ToIP Governance Stack

Layer 1

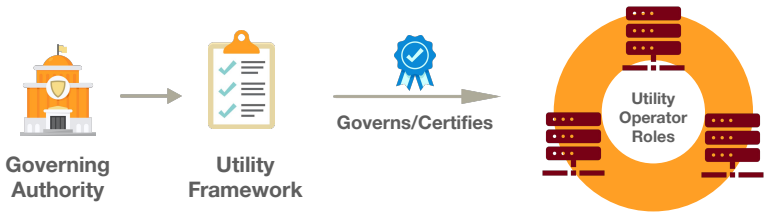
ToIP Technology Stack

ToIP Governance Stack

Public Utilities



Utility Governance Frameworks

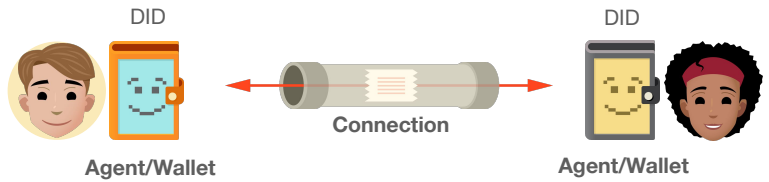


ToIP Technology Stack

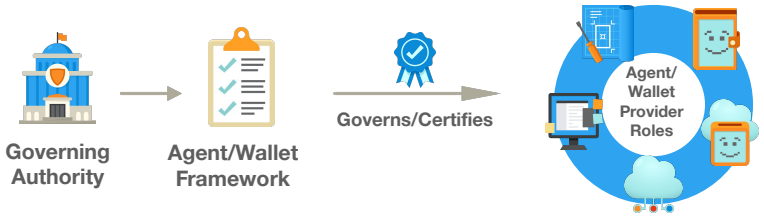
ToIP Governance Stack

Layer 2

Peer-to-Peer Communication

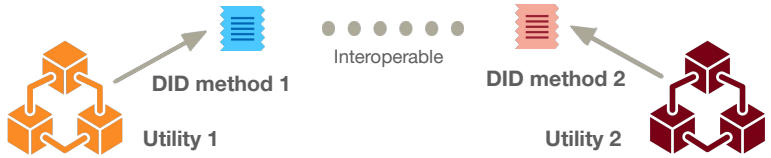


Agent/Wallet Governance Frameworks

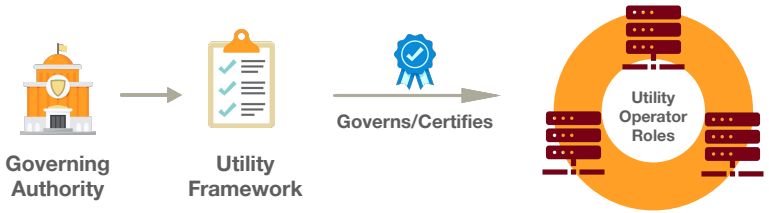


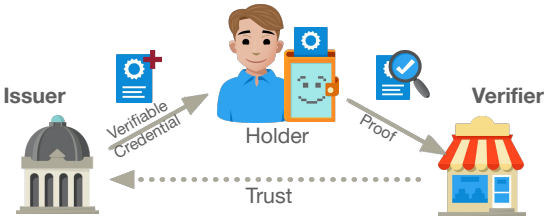
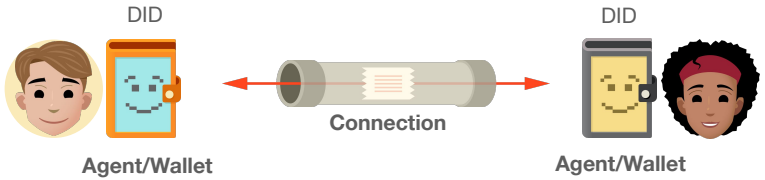
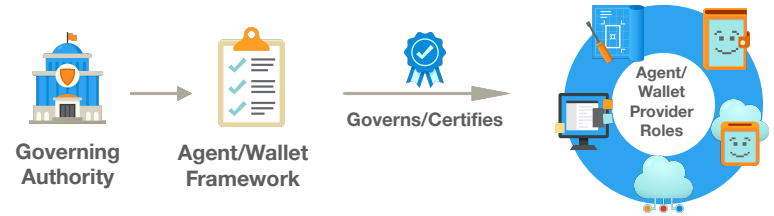
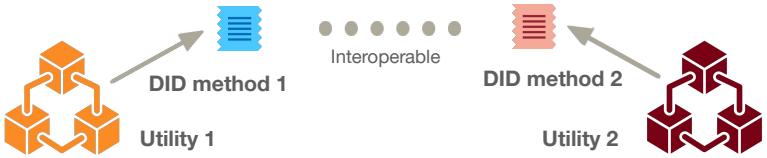
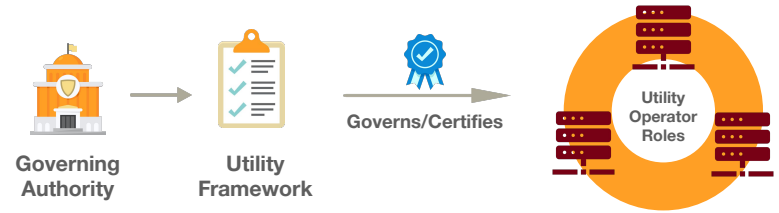
Layer 1

Public Utilities



Utility Governance Frameworks



	ToIP Technology Stack	ToIP Governance Stack
	Trust Task Protocols	Trust Task Governance Frameworks
Layer 3	Example: Credential Exchange 	
	Peer-to-Peer Communication	Agent/Wallet Governance Frameworks
Layer 2		
	Public Utilities	Utility Governance Frameworks
Layer 1		

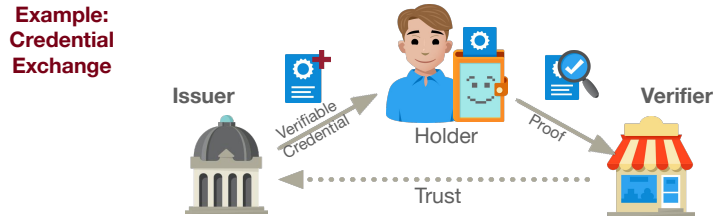
ToIP Technology Stack

Layer 4

Application Ecosystems

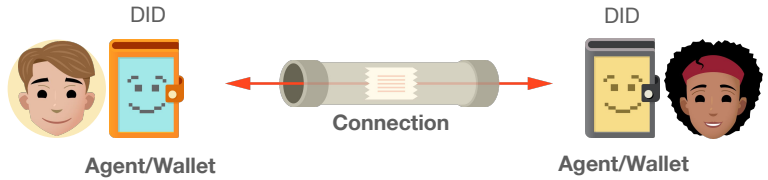
Layer 3

Trust Task Protocols



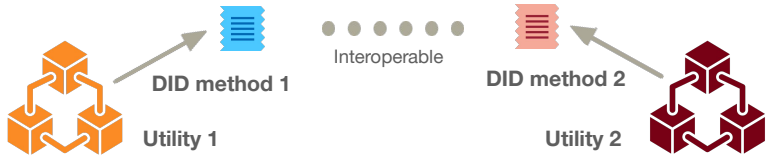
Layer 2

Peer-to-Peer Communication



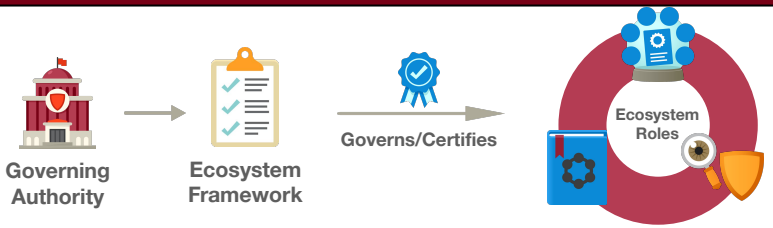
Layer 1

Public Utilities



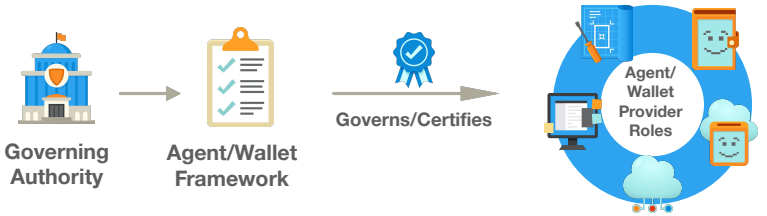
ToIP Governance Stack

Ecosystem Governance Frameworks



Trust Task Governance Frameworks

Agent/Wallet Governance Frameworks



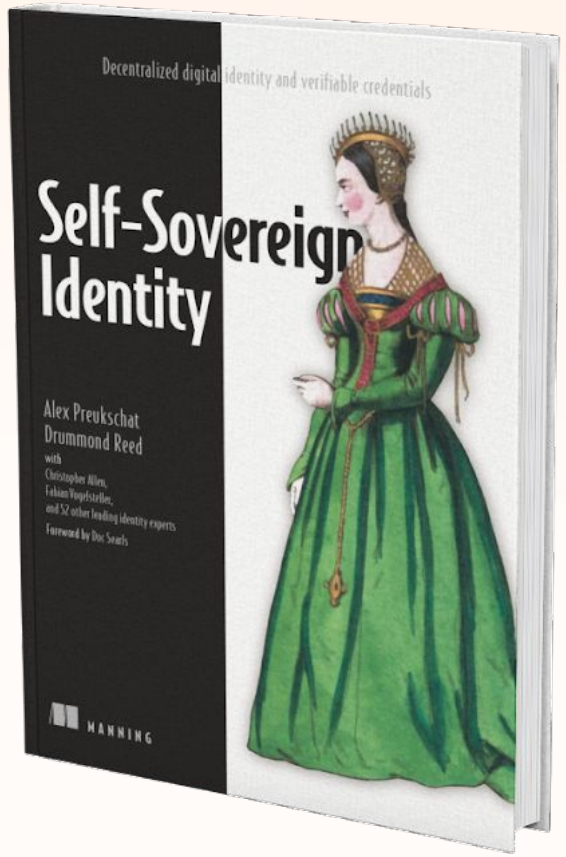
Utility Governance Frameworks

ToIP Working Groups

- Governance Stack WG
- Technology Stack WG
- Utility Foundry WG
- Ecosystem Foundry WG
- Concepts & Terminology WG
- Inputs & Semantics WG
- Human Experience WG
- Good Health Pass WG

If you'd like to learn more...

- The Book on Self-Sovereign Identity: https://www.manning.com/books/self-sovereign-identity
- Evernym webinar series: www.evernym.com/webinars/
- Blog post: The Inevitable Return to Self-Sovereign Identity
- Blog post: The Three Pillars of SSI
- Blog post: A Gentle Introduction to Verifiable Credentials
- Trust over IP: www.trustoverip.org




Avast