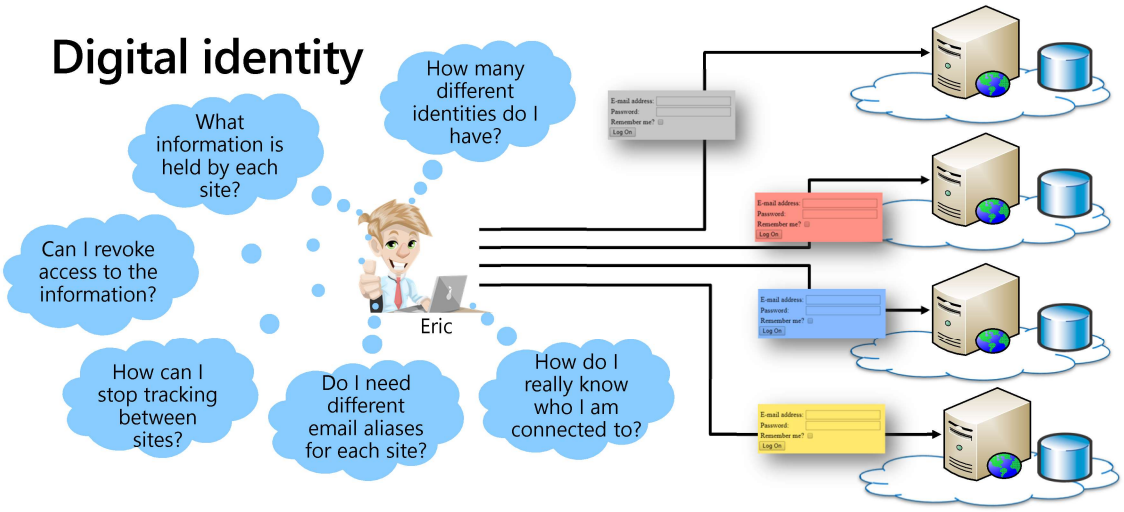
1

Decentralized Identity: one year on and counting

John Craddock
XTSeminars
Identity and security architect
www.xtseminars.co.uk, @john_craddock

2

Digital identity

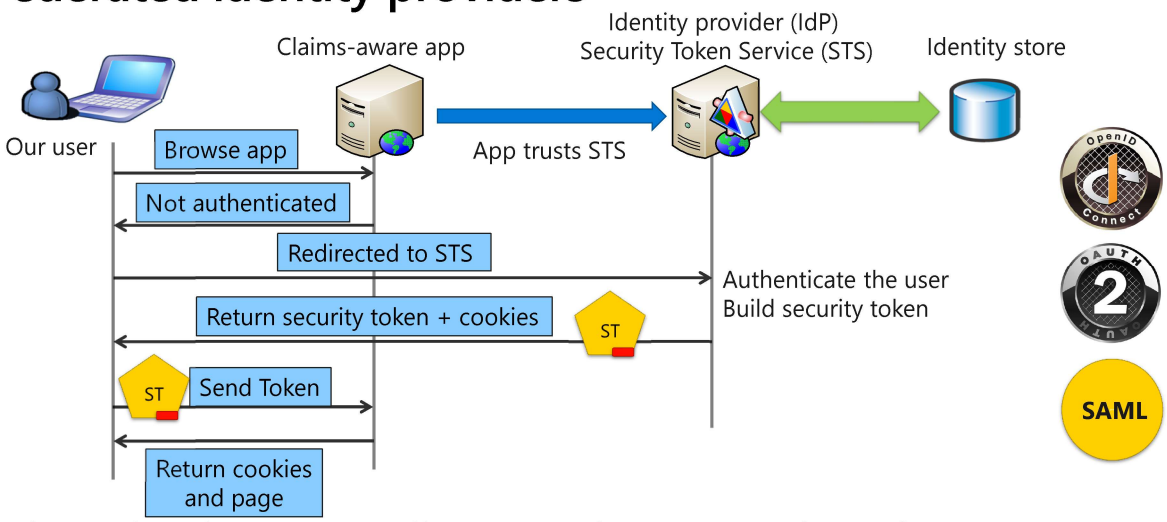


- Today our digital identity is held by many diverse and distributed organizations and websites
  - These entities are now custodians of our identity

XTSeminars

3

Federated identity providers



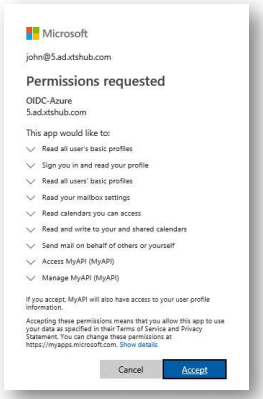
- Federated authentication allows one identity provider to factor authentication services to multiple entities

XTSeminars

4

Are we better off with federation?

- Our life just got easier
  - SSO to the IdP providing authentication to all services that trust that IdPPrivacy issues
- Privacy
  - We can now be easily tracked across different applications
  - How do we know/control what data is shared with different applications?
  - How can we revoke that shared information?
- Censorship
  - Our IdP could restrict what we can access or block our account



XTSeminars

5

Knowing who you are?

I'm eric@xtseminars.co.uk

Respond to this email to prove it

I'm over 18

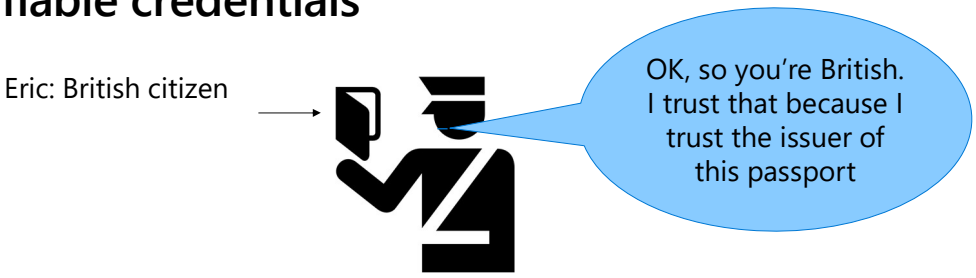
Give me you credit card details to prove it

- Claims/credentials are assertions about the user
- How do we prove that these assertions are true?
  - An organization may require additional verifiable data to be submitted
    - A utility bill or bank statement as proof of address
    - Notarised copies of your passport, driving licence, diploma, etc
- We invariably give away more information than we want to

XTSeminars

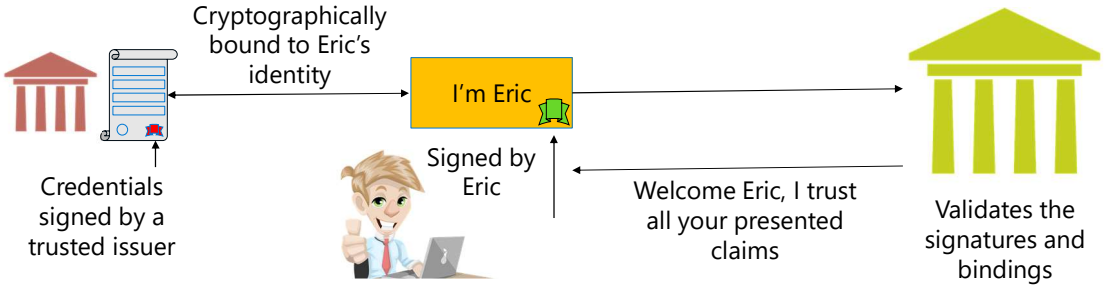
6

Verifiable credentials

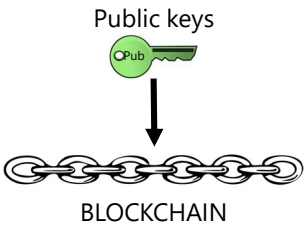


- Verifiable credentials are claims that are asserted by a fully trusted body
  - Also referred to as attestations and verifiable claims
- How do we verify that a presented credential or the envelop has not been forged?
- How do we digitally send verifiable credentials
  - A scanned copy of your passport won't do

How do we fix this?



- How does the organization validate the signatures?
  - They need the public keys that match the private signing keys
- Each entity self-issues a private/public key pair
  - Securely store the private key
  - Store the public key in an immutable decentralized ledger
- Locate the keys using a Digital ID (DID)



Decentralized identity is a work in progress

DIF

W3C®

IETF®

OASIS

- Many people and organizations involved
- Open source
- Standards are in development

DIF = Decentralized Identity Foundation
W3C = World Wide Web Consortium
IETF = Internet Engineering Task Force
OASIS = Organization for the Advancement of Structured Information Standards

9

XTSeminars

DIF membership keeps growing

XTSeminars

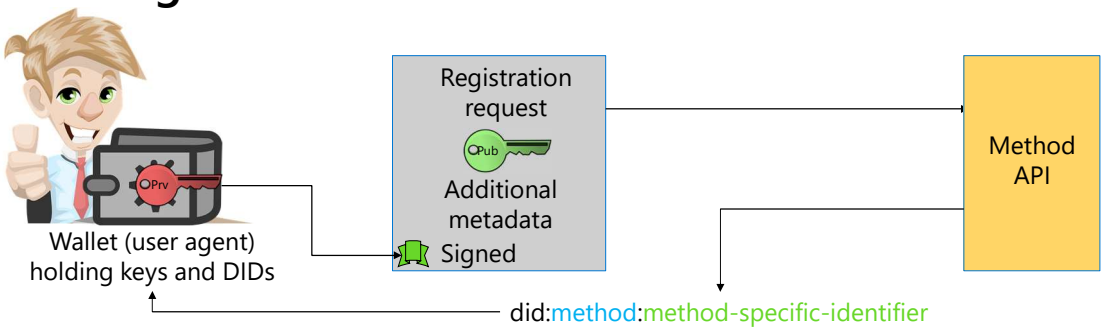
uPort donates code

- In November 2019 it was announced that uPort has donated much of its core libraries to DIF
- uPort were co-founders of DIF
- Goal of donating the libraries was to make it easier for developers to create standards-based identity applications

11

11

DID Registration

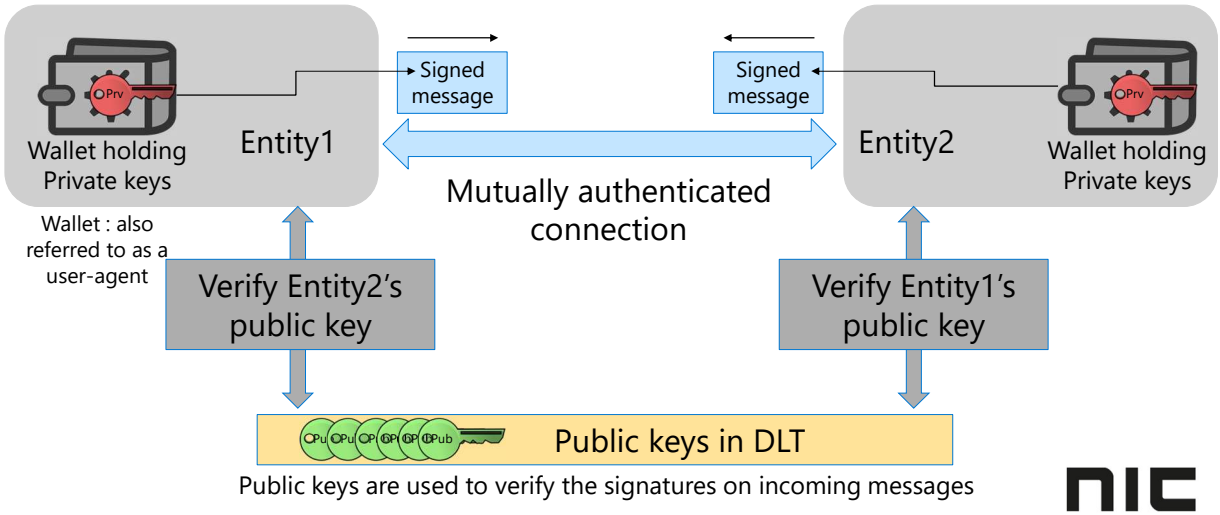


- To register a DID you will need a public/private key pair
- Your private key will remain in your wallet and your public key will be stored in the blockchain
- A trusted, tamper-evident public key ledger
  - Keys accessible via the DID

12

12

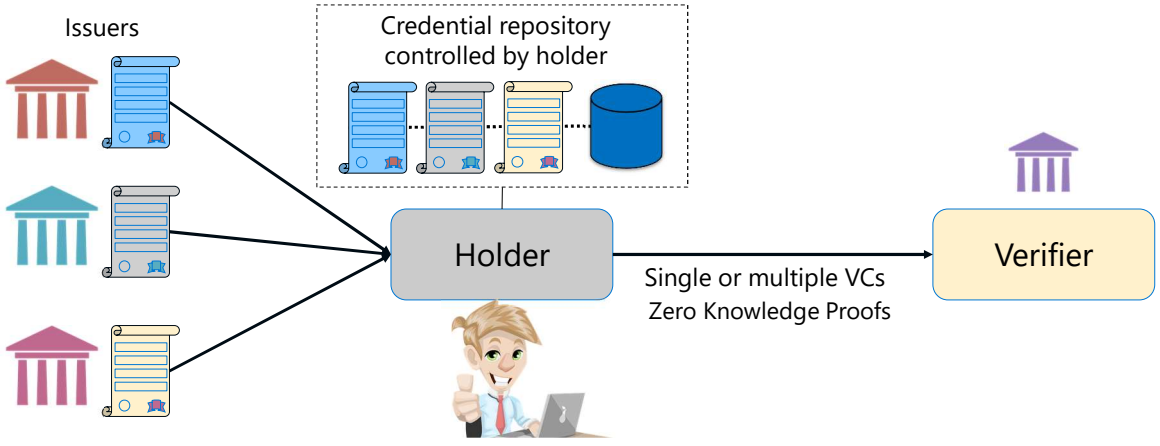
Peer-to-Peer connections



DLT = Decentralized Ledger Technology

13

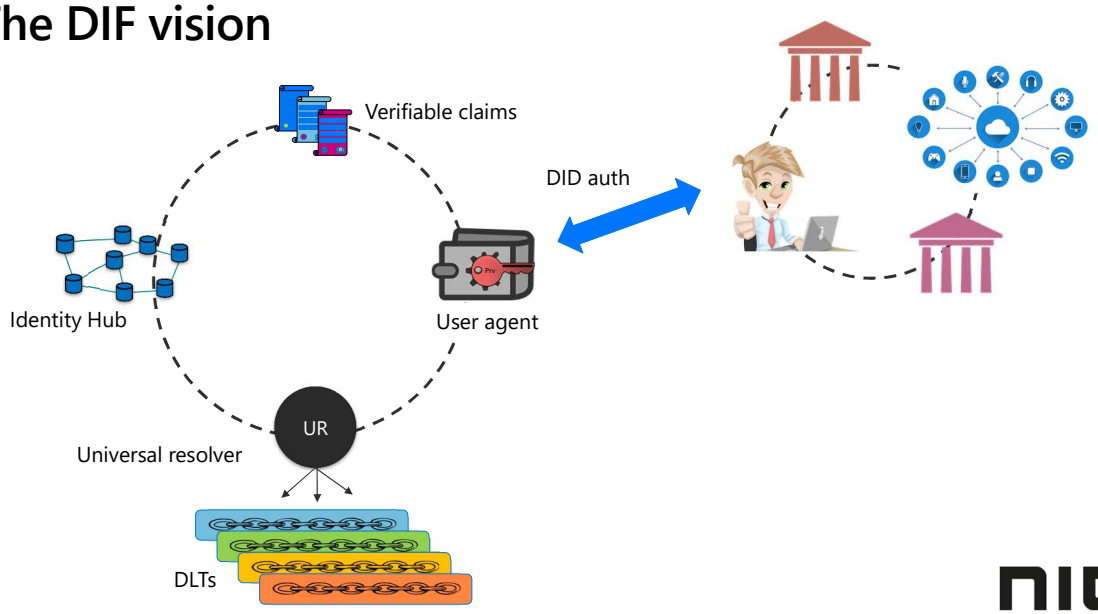
VCs from multiple resources



- All credentials can be checked that they were issued to Eric and that they have not been revoked

14

The DIF vision



XTSeminars

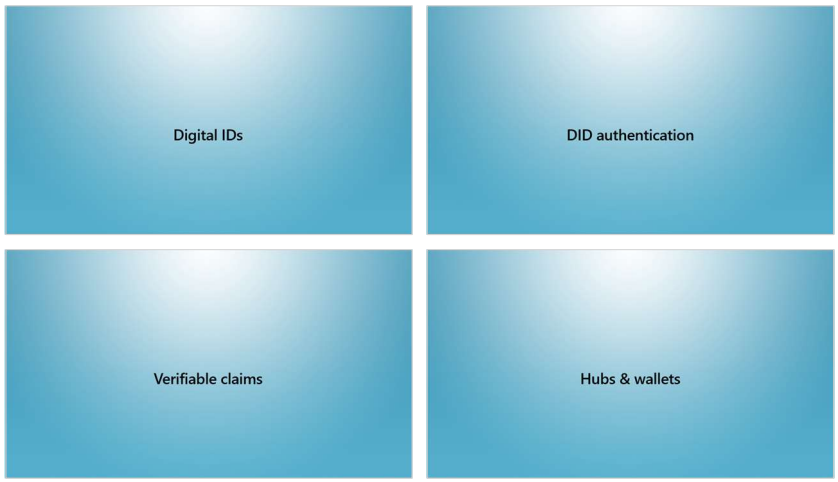
15

Self-Sovereign Identity becomes a reality

- Who is in control of your identity?
  - Only you, no central authority
- Who can take it away or censor it?
  - No one
- How many identities will you have?
  - As many as needed
- What types of identity can be stored?
  - Identity for: users, organizations, devices, applications, IOT
- Do I have to register my life with every different entity to gain access?
  - No, obtain verifiable claims once and use cryptographic proofs everywhere
- Can I restrict how much information I disclose
  - Yes
- Can I easily revoke access to that information
  - Yes

XTSeminars

Let's break it down



XTSeminars

17

Digital IDs

18

Requirements of a DID

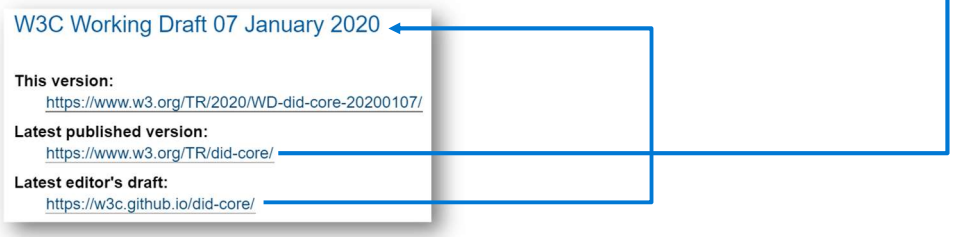
- Decentralized
  - No central issuing authority
- Persistent
  - Not requiring the continued operation of any underlying agencies
- Cryptographically verifiable
- Resolvable to DID document

XTSeminars

19

Decentralized Identifiers (DIDs) v1.0

- W3C Working Draft 09 December 2019
  - All standards and drafts can be found here https://www.w3.org/TR/
- It can get confusing!

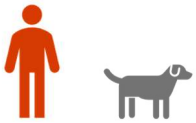


XTSeminars

20

DIDs

Controller and subject



Controller Subject

Controller Subject

- DIDs are URIs that relate a subject to a DID document
- A DID document allows cryptographically-verifiable interactions with the subject and can include
  - Subject ID
  - Controller ID
  - Public Keys
  - Authentication methods
  - Service endpoints

XTSeminars

21

DID Document format (JSON-LD)

```
{
    "@context": "https://www.w3.org/ns/did/v1",
    "id": "sov:WRfXPg8dantKVubE3HX8pw",
    "publicKey": [{  }],
    "authentication": [{  }],
    "service": [{  }]
}
```

Public key associated with DID private key

How to authenticate as DID

Endpoint to retrieve other data associated with the DID

XTSeminars

22

Resolving a DID to a DID document

did:method:method-specific-identifier

- Depending on the underlying DTL the DID document may be fully or partially held on the Ledger
  - The details of Creating, Reading, Updating and Deleting (CRUD) are defined by the DID method
- The crypto components (public keys) will always be held by the DLT
- Examples:
  - Sovrin holds the full DID on-chain
  - Bitcoin can only hold limited data and the service endpoints are referenced via an off-chain document.

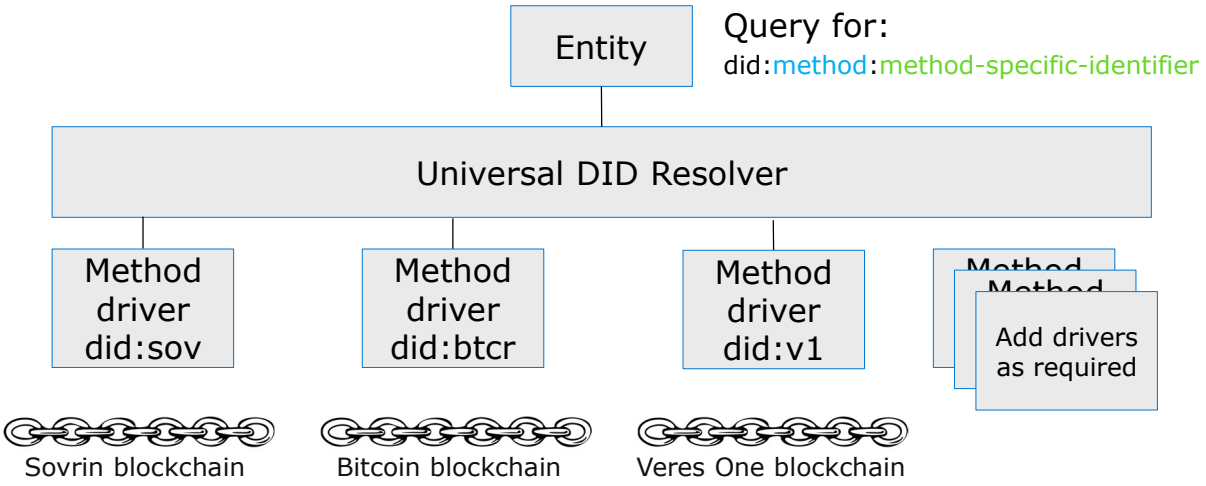
XTSeminars

40+ different methods in progress

Method Name	Status	DLT or Network	Authors	Link
did:abt:	PROVISIONAL	ABT Network	ArcBlock	ABT DID Method
did:btcr:	PROVISIONAL	Bitcoin	Christopher Allen, Ryan Grant, Kim Hamilton Duffy	BTCR DID Method
did:stack:	PROVISIONAL	Bitcoin	Jude Nelson	Blockstack DID Method
did:erc725:	PROVISIONAL	Ethereum	Markus Sabadello, Fabian Vogelsteller, Peter Kolarov	erc725 DID Method
did:example:	PROVISIONAL	DID Specification	W3C Credentials Community Group	DID Specification
did:ipid:	PROVISIONAL	IPFS	TranSendX	IPID DID method
did:life:	PROVISIONAL	RChain	lifeID Foundation	lifeID DID Method
did:sov:	PROVISIONAL	Sovrin	Mike Lodder	Sovrin DID Method
did:uport:	DEPRECATED	Ethereum	uPort	
did:ethr:	PROVISIONAL	Ethereum	uPort	ETHR DID Method
did:v1:	PROVISIONAL	Veres One	Digital Bazaar	Veres One DID Method
did:com:	PROVISIONAL	commercio.network	Commercio Consortium	Commercio.network DID Method
did:dom:	PROVISIONAL	Ethereum	Dominode	
did:ont:	PROVISIONAL	Ontology	Ontology Foundation	Ontology DID Method
did:vvo:	PROVISIONAL	Vivvo	Vivvo Application Studios	Vivvo DID Method
did:aergo:	PROVISIONAL	Aergo	Blocko	Aergo DID Method
did:icon:	PROVISIONAL	ICON	ICONLOOP	ICON DID Method
did:iwt:	PROVISIONAL	InfoWallet	Raonsecure	InfoWallet DID Method
did:ockam:	PROVISIONAL	Ockam	Ockam	Ockam DID Method
did:ala:	PROVISIONAL	Alastria	Alastria National Blockchain Ecosystem	Alastria DID Method
did:op:	PROVISIONAL	Ocean Protocol	Ocean Protocol	Ocean Protocol DID Method
did:jlinc:	PROVISIONAL	JLINC Protocol	Victor Grey	JLINC Protocol DID Method
did:ion:	PROVISIONAL	Bitcoin	Various DIF contributors	ION DID Method
did:jolo:	PROVISIONAL	Ethereum	Jolocom	Jolocom DID Method
did:bryk:	PROVISIONAL	bryk	Marcos Allende, Sandra Murcia, Flavia Munhoso, Ruben Cessa	bryk DID Method
did:peer:	PROVISIONAL	peer	Daniel Hardman	peer DID Method
did:selfkey:	PROVISIONAL	Ethereum	SelfKey	SelfKey DID Method
did:meta:	PROVISIONAL	Metadium	Metadium Foundation	Metadium DID Method
did:tys:	PROVISIONAL	DID Specification	Chainyard	TYS DID Method
did:git:	PROVISIONAL	DID Specification	Internet Identity Workshop	Git DID Method
did:tangle:	PROVISIONAL	IOTA Tangle	BiiLabs Co., Ltd.	TangleID DID Method
did:emtrust:	PROVISIONAL	Hyperledger Fabric	Halialabs Pte Ltd.	Emtrust DID Method
did:ttm:	PROVISIONAL	TMChain	Token.TM	TM DID Method
did:wlk:	PROVISIONAL	Weelink Network	Weelink	Weelink DID Method
did:pistis:	PROVISIONAL	Ethereum	Andrea Taglia, Matteo Sinico	Pistis DID Method
did:holo:	PROVISIONAL	Holochain	Holo.Host	Holochain DID Method
did:web:	PROVISIONAL	Web	Oliver Terbu, Mike Xu, Dmitri Zagidulin, Amy Guy	Web DID Method
did:io:	PROVISIONAL	IoTeX	IoTeX Foundation	IoTeX DID Method
did:vaultie:	PROVISIONAL	Ethereum	Vaultie Inc.	Vaultie DID Method
did:moac:	PROVISIONAL	MOAC	MOAC Blockchain Tech, Inc.	MOAC DID Method
did:omn:	PROVISIONAL	OmniOne	OmniOne	OmniOne DID Method
did:work:	PROVISIONAL	Hyperledger Fabric	Workday, Inc.	Workday DID Method
did:vid:	PROVISIONAL	VP	VP Inc.	VP DID Method
did:ccp:	PROVISIONAL	Quorum	Baidu, Inc.	Cloud DID Method
did:jnctn:	PROVISIONAL	Jnctn Network	Jnctn Limited	JNCTN DID Method
did:elastos:	PROVISIONAL	Elastos ID Sidechain	Elastos Foundation	Elastos DID Method

XTSeminars

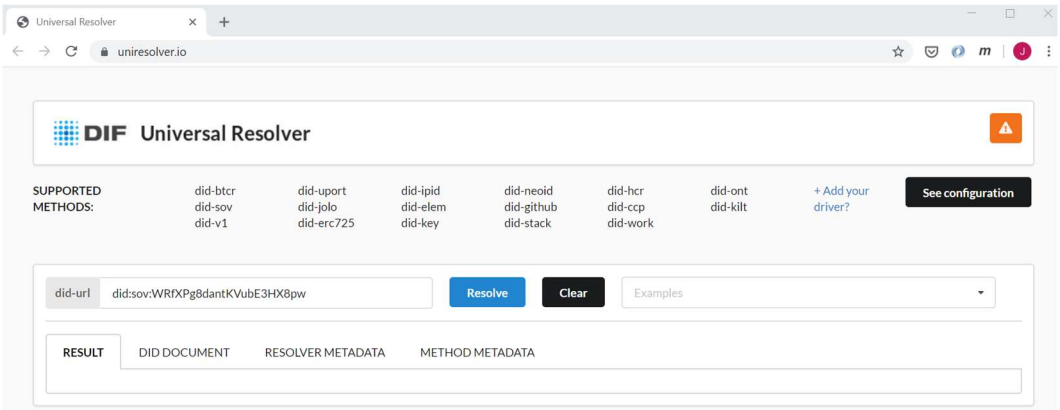
Universal DID Resolver



XTSeminars

25

DIF Universal resolver



XTSeminars

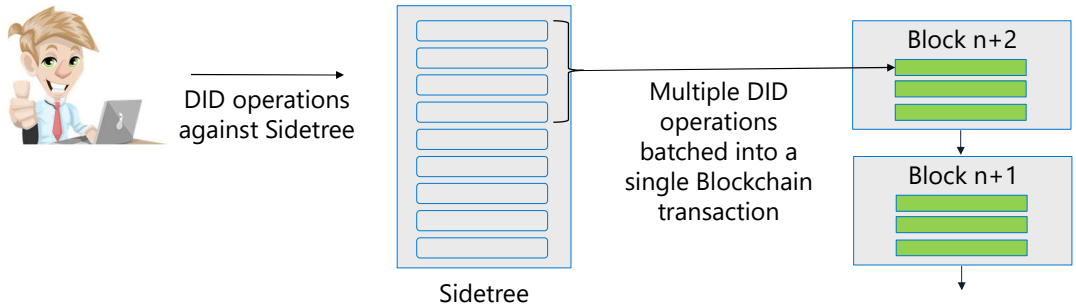
Blockchain performance

- The time from generating a transaction until it is confirmed can take a considerable time
  - On the Bitcoin Blockchain transactions are mined every 10 minutes
    - There is no guarantee that your transaction and hence the DID will be added to the next block
- Sidetree is a protocol that can be added to any to any DLT
  - It creates a layer 2 PKI network capable of managing tens of thousands operations/second
  - DID methods will interact with Sidetree
    - The method symbol is "ion"
- Development code available via Github

27

XTSeminars

Sidetree



- Blockchain provides the immutability and verification guarantees
  - DID operations are stored in a batch file
    - Data held in Distributed Content-Addressable Storage (DCAS)
  - Merkle tree root of the operation hashes are stored into blockchain

28

XTSeminars

DIF: Well Known DID Configuration

Identity.foundation/.well-known/did-configuration

```
{
   entries: [
      {
         did: "did:btcr:xxcl-lzpq-q83a-0d5",
         jwt: "eyJhbGciOiJFUzI1NksiLCJ...
      }
    ]
}
```

```
{
  "alg": "ES256K",
  "kid": "JUvpllMEYUZ2joO59UNui_XYDqxVqiFLLAJ8klWuPBw"
}.{
  "iss": "did:btcr:xxcl-lzpq-q83a-0d5",
  "domain": "identity.foundation",
  "exp": 1928930300,
  "iat": 1568933900
}.[Signature]
```

- Provides method for finding the DID for Internet domains
- JWT signed by private key associated with DID

XTSeminars

DID authentication

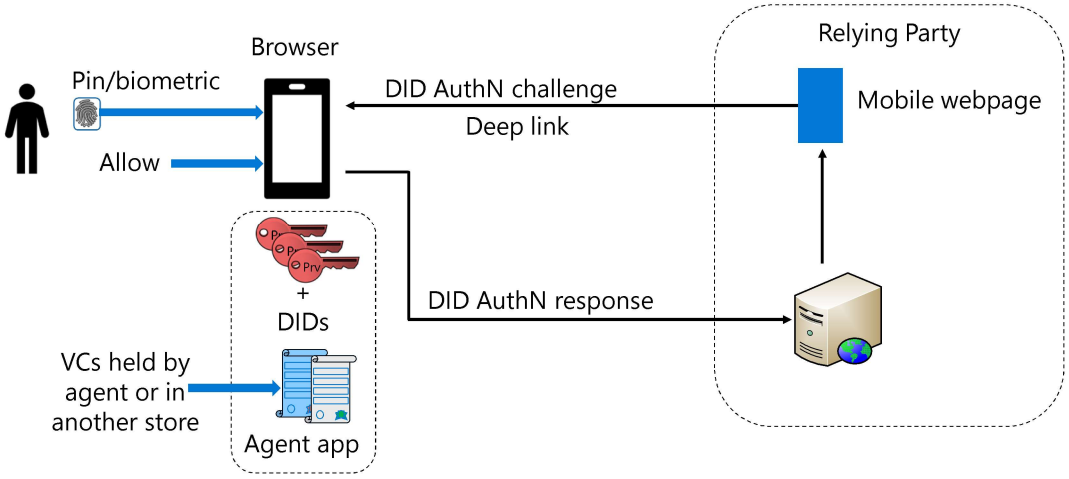
DID Authentication

- DIF working draft for a Self-Issued OpenID Connect Provider DID Profile (SIOP DID Profile or SIOP DID)
  - In the meantime many vendors have created their own or adapted existing protocols
- Built on the Self-Issued OpenID Provider (OP) which is part of the core OpenID Connect standard
  - https://openid.net/specs/openid-connect-core-1_0.html (Section 7)
  - Allows a personal self-hosted OP to issue self-signed ID Tokens
  - The issuer is https://self-issued.me
- OP could be via a mobile, web browser extension of hardware device
- Support for different authentication architectures

XTSeminars

31

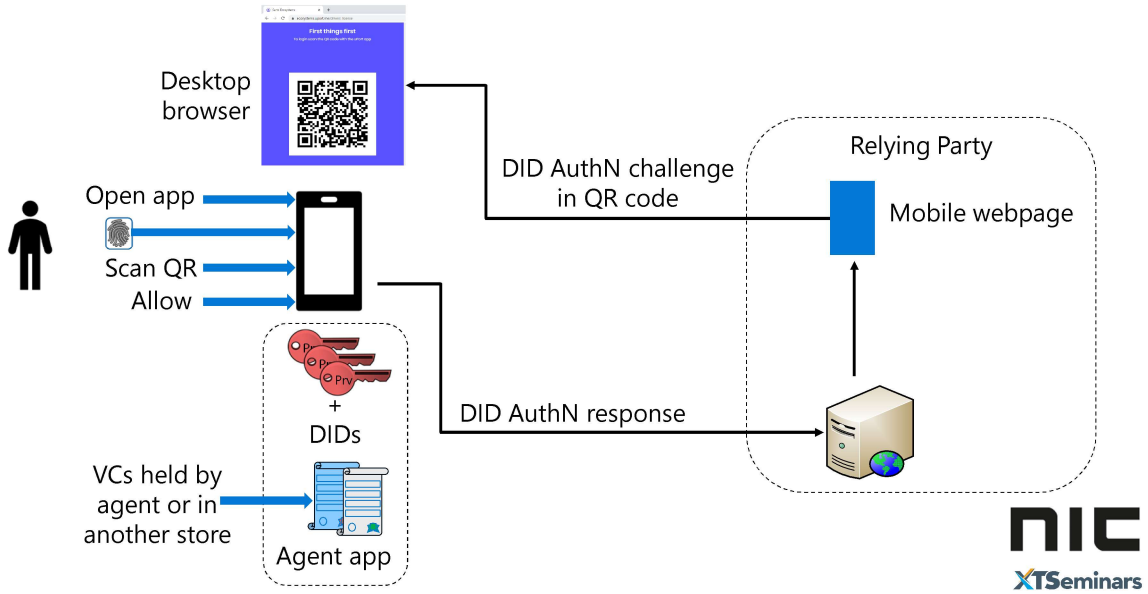
Example 1: mobile browser and mobile agent



XTSeminars

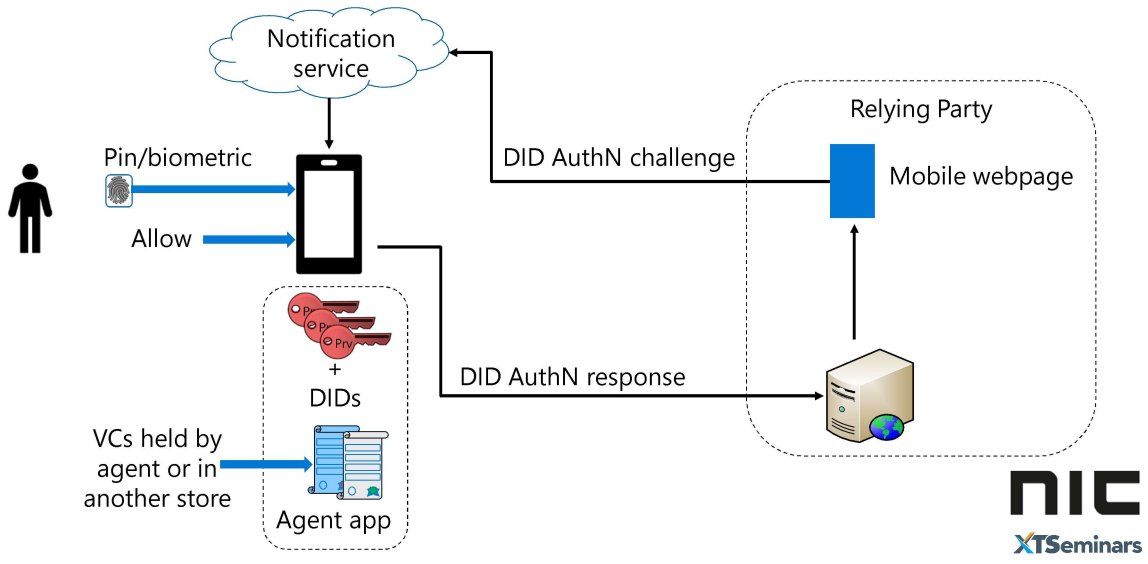
32

Desktop browser and mobile agent



33

Desktop browser and mobile agent v2



34

Verifiable claims

35

Public versus Private identities

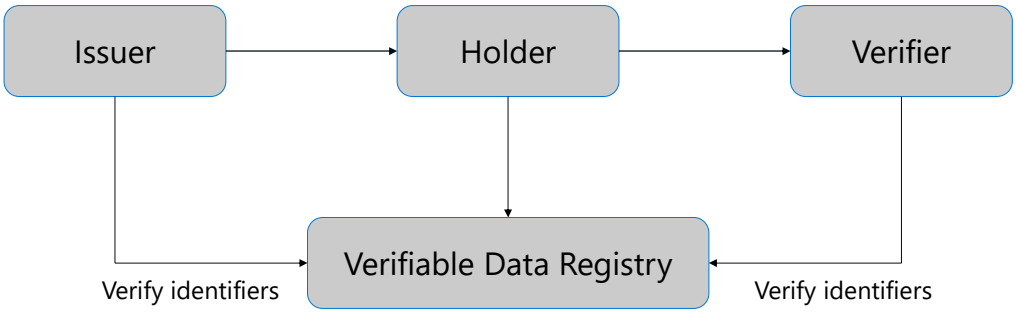
- Public identities are essential for trusting
  - Organizations issuing verifiable claims
  - Organizations providing services to us
  - Users needing to publish information that they want publicly available and verifiable to them
- In most situations a user will not want a public identity with which to transact their business
  - Pseudo anonymous pairwise identities can be created for each service the user is required to authenticate to
    - The identity consists of a new private/public pair created for each service
    - Verifiable credentials are cryptographically bound to the identities

36

XTSeminars

36

Verifiable credentials



- For privacy it is important that the Verifier does not query the issuer to validate credentials

XTSeminars

37

Verifiable Credentials Data Model 1.0

- Standardizing a data model for VCs
  - Specified in JSON-LD
  - Allows any type of cryptography to protect it
- Protocols to handle VCs currently out of scope
  - Vendors are going there own way

XTSeminars

Example VC from W3


```
"verifiableCredential": [{
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/1634",
    "type": ["VerifiableCredential", "AlumniCredential"],
    "issuer": "https://example.edu/issuers/540967",
    "issuanceDate": "2020-01-01T18:73:24Z",
    "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "alumniOf": {
        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
        "name": [{
          "value": "Example University",
          "lang": "en"
        }, {
          "value": "Exemple d'Université",
          "lang": "fr"
        }]
      }
    },
    "proof": {...}
  }],
```


- @context maps globally unique identifiers to user friendly alias

Claims from an IdP

- IdP holds a limited set of data about the user
- Trust is with the IdP that asserts the claim
  - How do you know the claim is up-to-date?
- IdP is in control of what it releases to an RP
  - May release more information than a user wants given to an RP
  - May refuse to release information required
- The RP may require attributes from multiple authorities
  - For correlation the user would require a globally unique identify
    - Tracking and privacy concerns

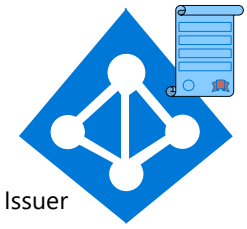
Verifiable credentials from an issuer

- The required VCs can be gathered from multiple authorities
- Trust is with the issuing authority
- VC can be verified for revocation
- The issuing of all VCs to a RP is under the control of the use
  - Zero-knowledge proofs reduce disclosure
- VCs can be issued to a RP individually, as a presentation (set) and from different issuing authorities
- The VCs are cryptographically bound to the Pairwise ID
  - Can not be stolen and used for impersonation

XTSeminars

41

Azure AD and verifiable claims



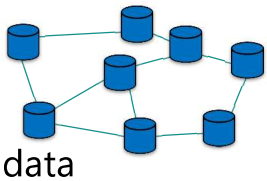
- Coming in 2020 all Azure AD tenants will become capable of issuing verifiable claims

XTSeminars

42

Hubs & wallets

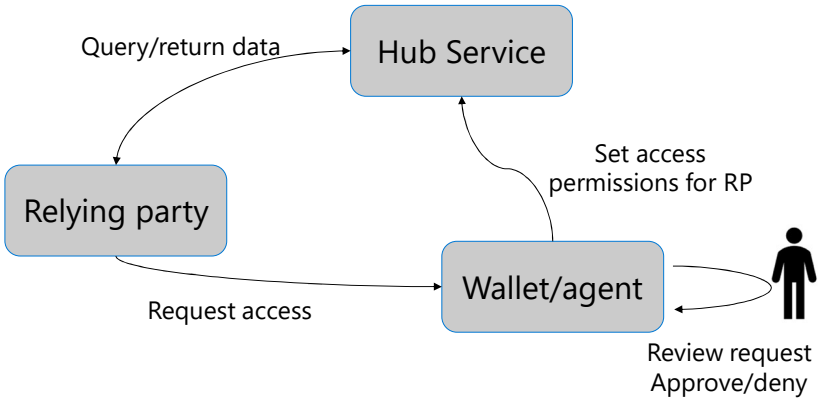
Off-chain storage



- DIF has proposed Identity Hubs for off-chain storage of data
  - A Hub is a datastore containing related data objects at well-known locations
  - Each object is signed by a DID
  - Hub instances synchronise via a P2P protocol
  - To allow access independently of the hub instance a URI schema will be used to identity the data
    - A hub may be an edge or cloud device
- DID Auth will be used to authenticate requests to the Hub
- Permissions, set by the owner of the data, control access
- Data should be easily exportable to ensure the entity has full control over the portability of their data

XTSeminars

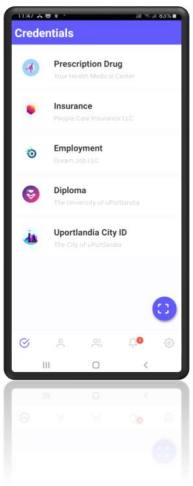
Hub Access



- At any time the user can deny the RP access to the data
- Hubs and wallets work together to manage identity, requesting/issuing claims and allowing access to other data

XTSeminars

Example Wallet



Wallet/user agent example
From uPort
https://uportlandia.uport.me/

XTSeminars

Demo…

uPort

47

Self-Sovereignty Rocks
In the math we trust

48

Join me for a masterclass

Identity masterclass

Auth Protocols Troubleshooting masterclass

Follow me!
@john_Craddock
www.xtseminars.co.uk

Public masterclasses: UK, The Netherlands, Switzerland, Norway, Sweden, Finland, USA
Onsite masterclasses: as requested

www.xtseminars.co.uk for details

XTSeminars