condatis
a sitekit company

Decentralized identity protocols and standards

Richard Astley, Solutions Architect

Mikko Vuorinen, Senior Developer

18th November 2020

protecting organisations, connecting people

condatis
a sitekit company

Previously

Last webinar

- Wallets
- Identity
- decentralized identity
- Trust between parties and the exchange of credentials

This webinar

- Standards
- Protocols
- Agents and Wallets
- Interoperability
- Condatis decentralised identity system, Condatis Staff Passport

condatis
a sitekit company

condatis
a sitekit company

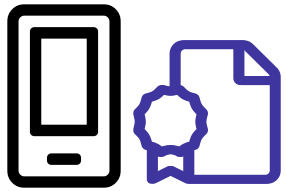
Verifiable Credentials

Overarching standards for Decentralized Identity

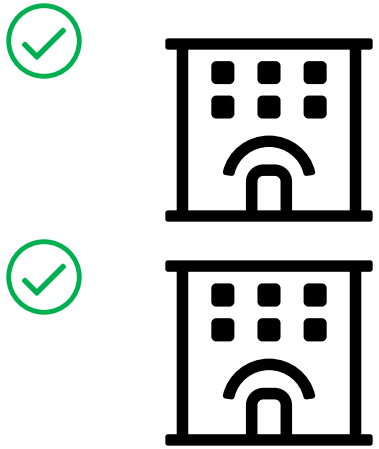
Verifiable Credentials Data Model

- Credential on Web www.w3.org/TR/vc-data-model
- Cryptographically secure, privacy respecting, machine-verifiable
- Claims, Credentials, Presentations

Issuer



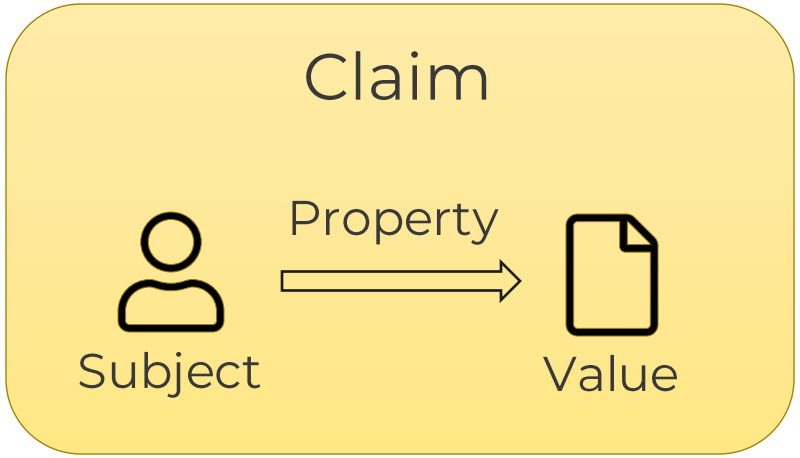
Holder



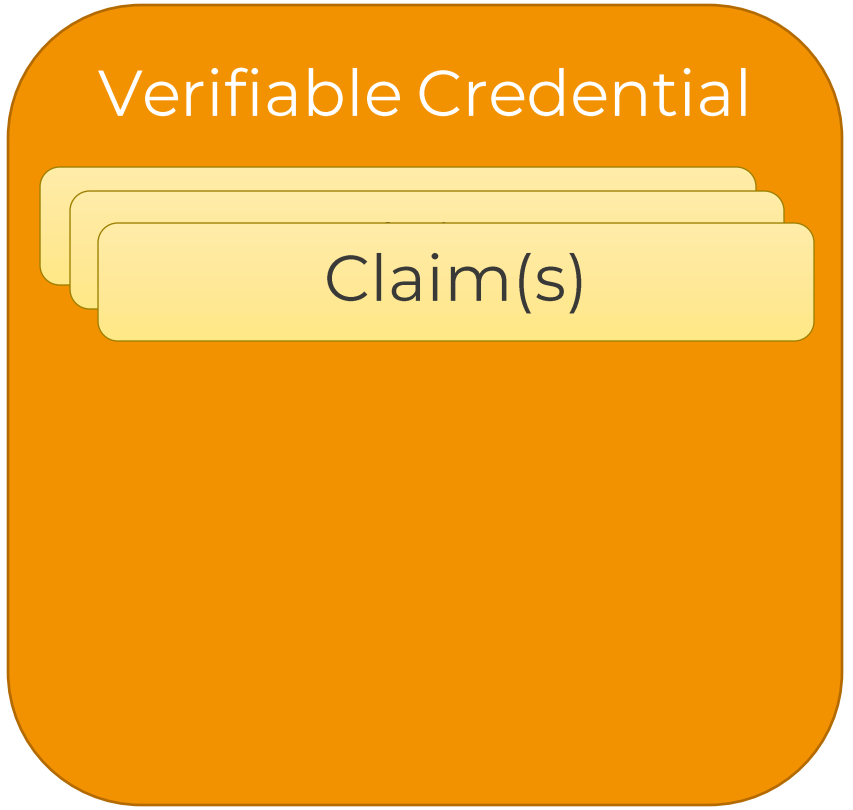
Verifiers

condatis
a sitekit company

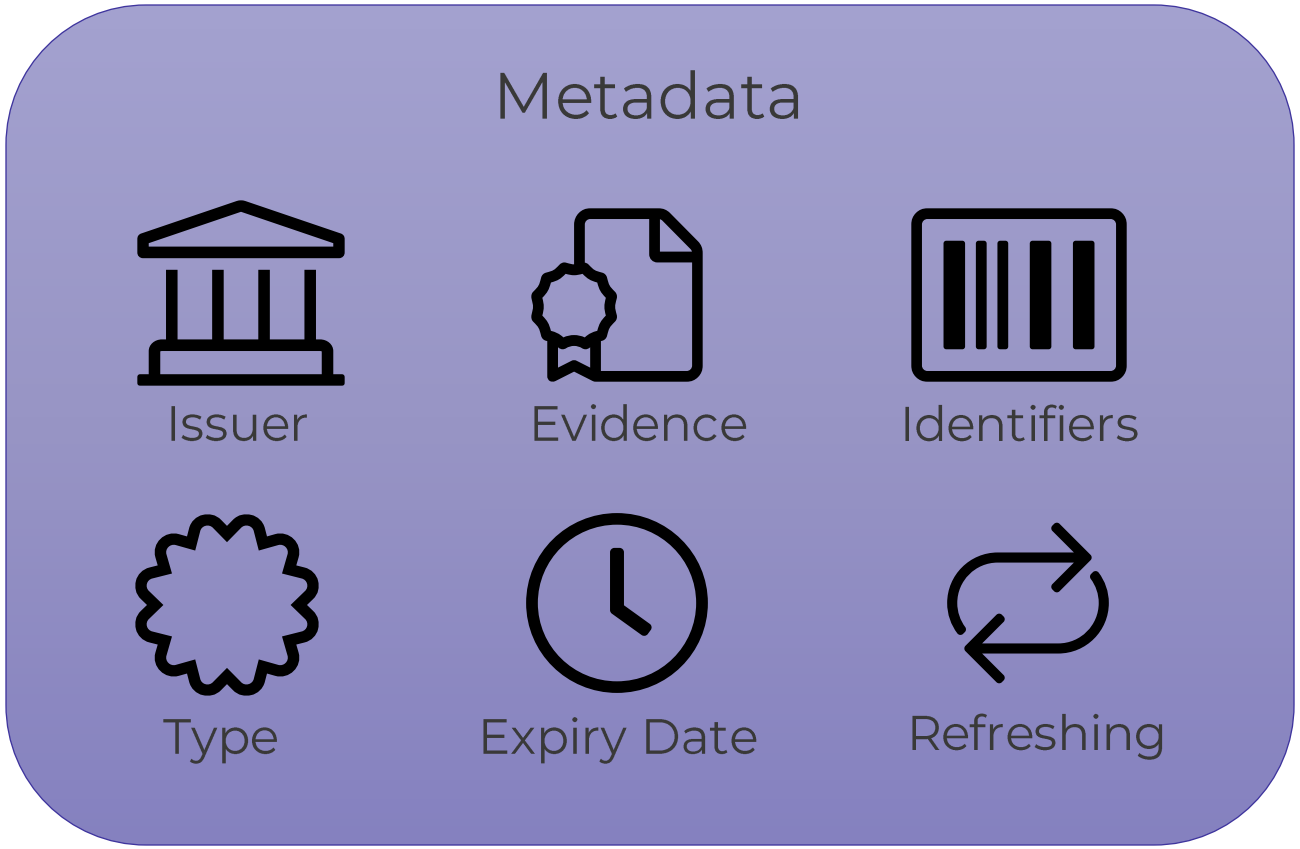
Verifiable Credential

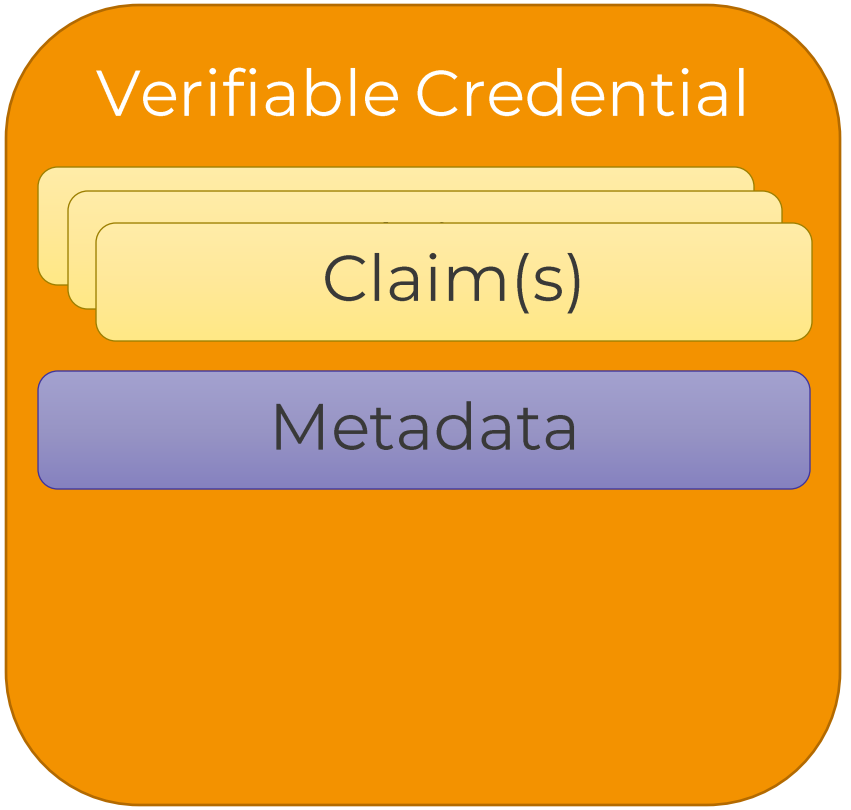


“Mikko works at Condatis”



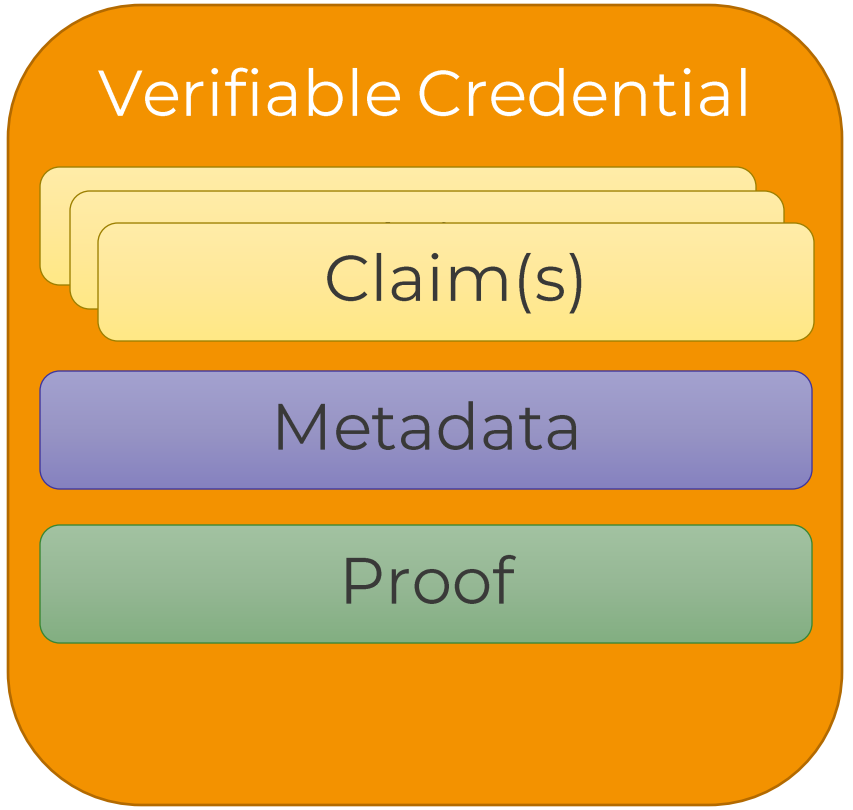
Verifiable Credential





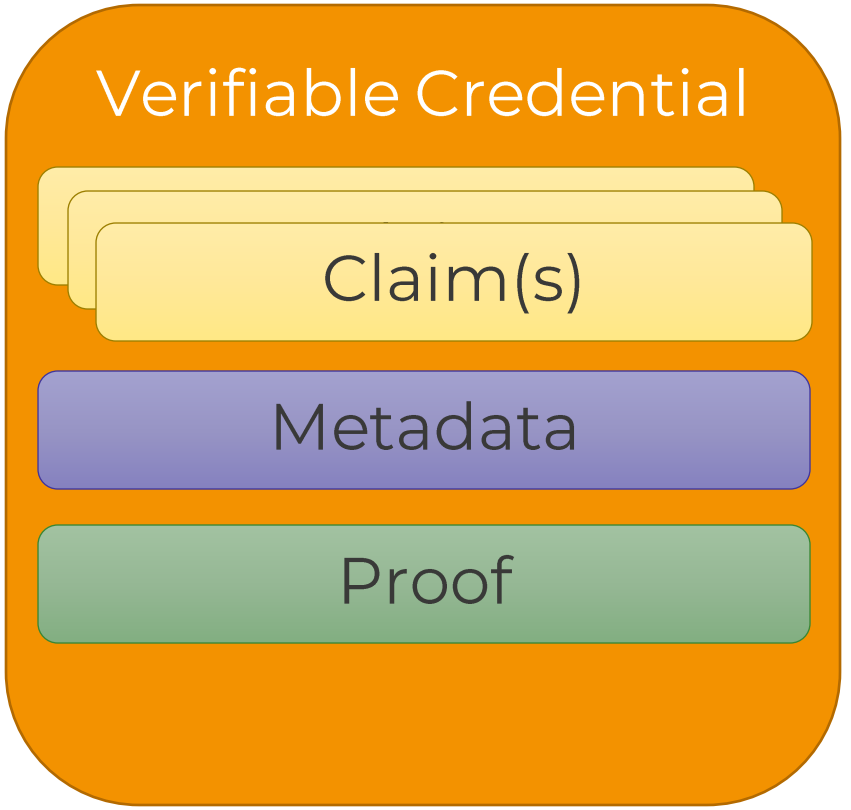
condatis
a sitekit company

Verifiable Credential



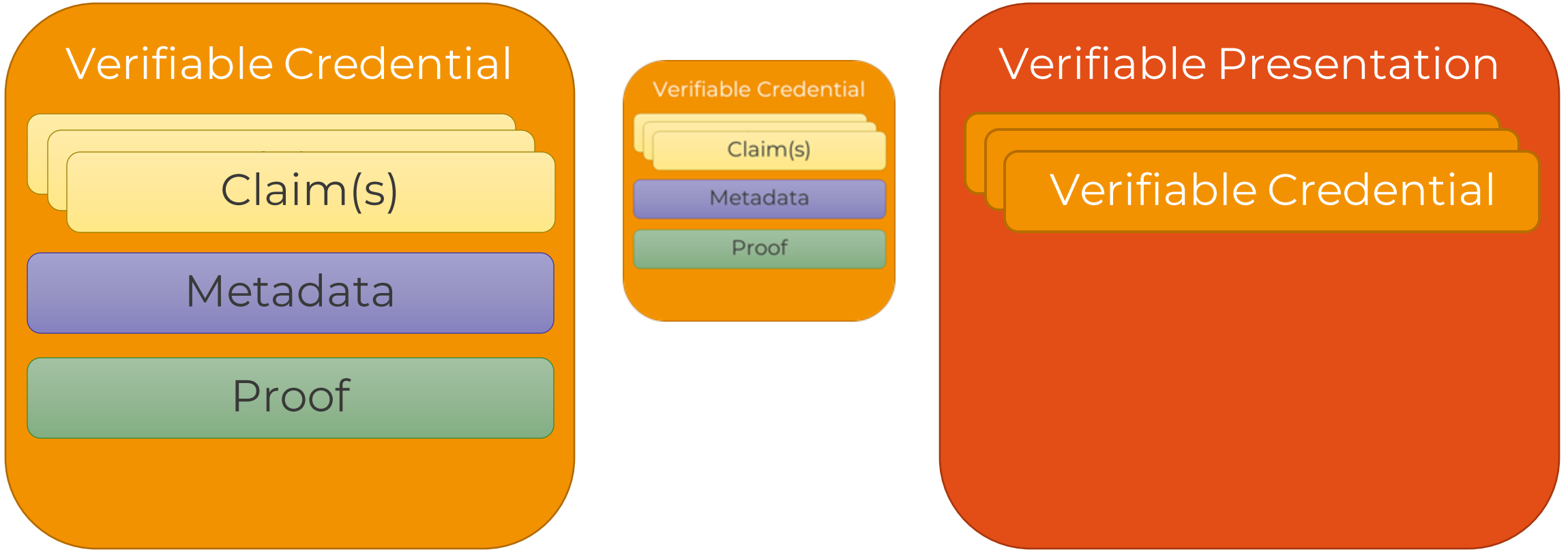
Verifiable Credential

```
{
    "@context": [ "https://www.w3.org/2018/credentials/v1" ],
    "id": "http://condatis.com/credentials/123",
    "type": [ "VerifiableCredential" ],
    "issuer": "https://condatis.com/issuers/001",
    "issuanceDate": "2020-11-18T12:00:00Z",
    "credentialSubject": {
        "id": "did:example:abc123",
        “worksAt": "Condatis"
    },
    "proof": {
        "type": "RsaSignature2018",
        "created": "2020-11-18T12:00:00Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod": "https://condatis.com/issuers/keys/1",
        "jws": "ey..."
    }
}
```

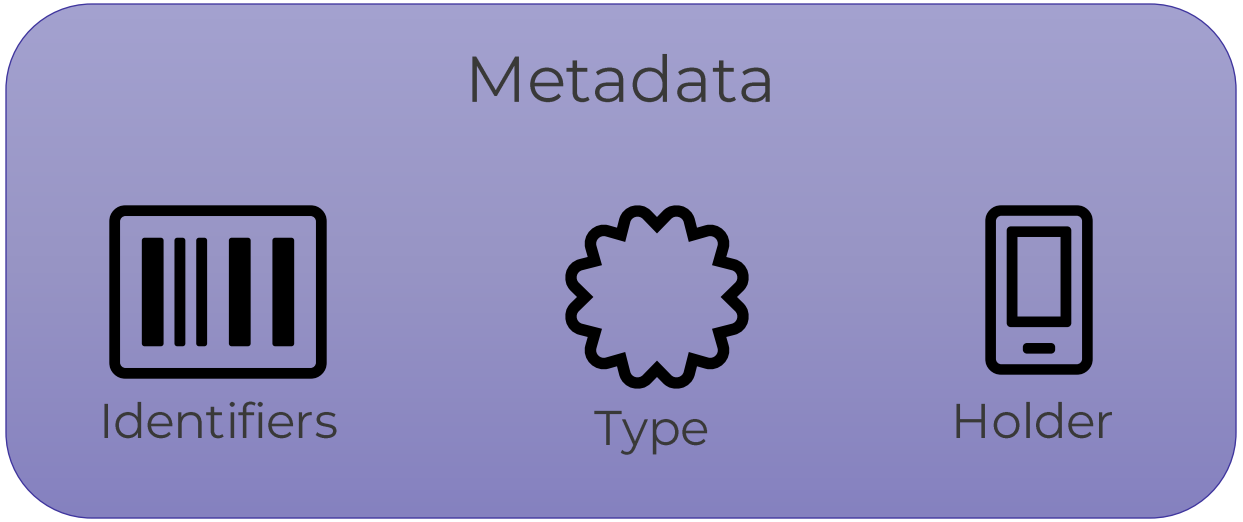


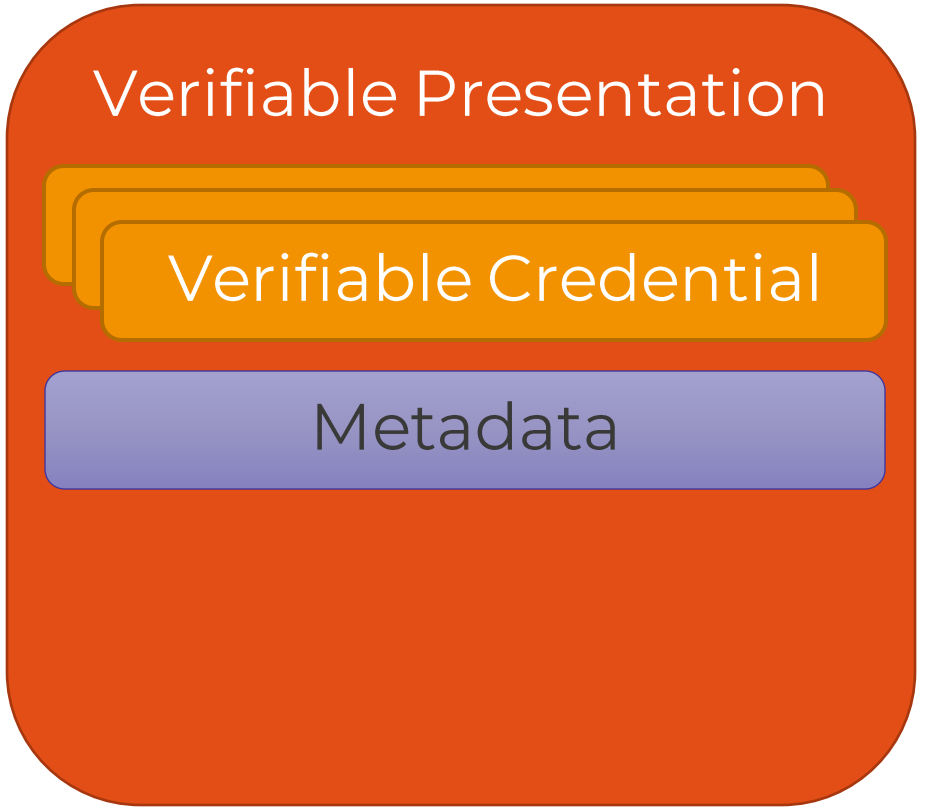
condatis
a sitekit company

Verifiable Presentation



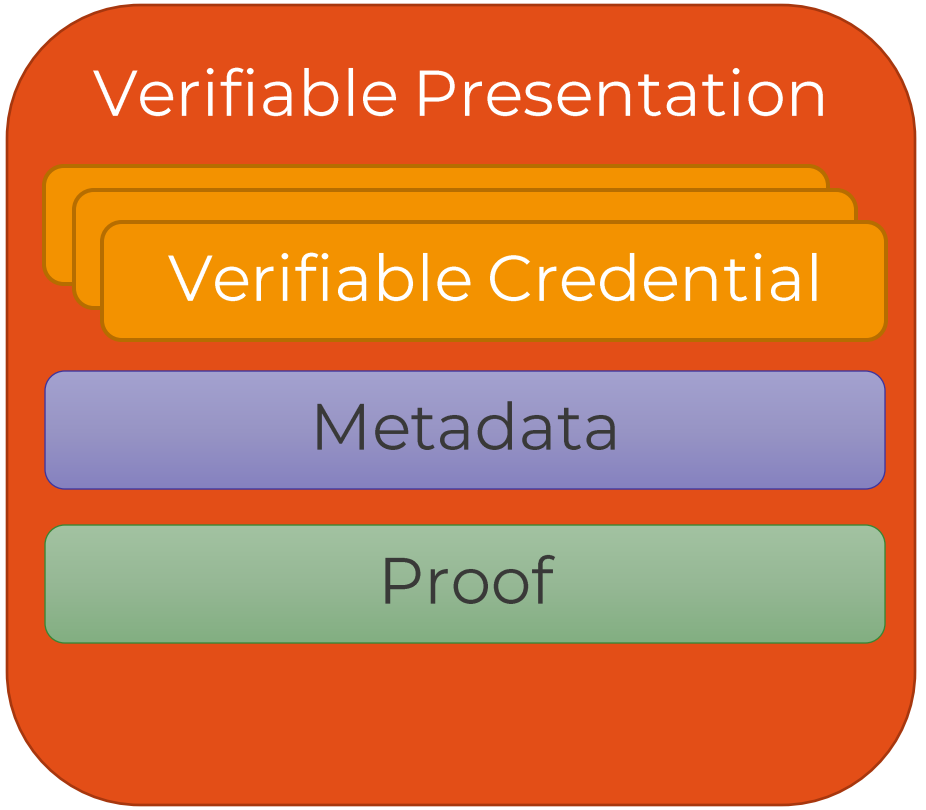
Verifiable Presentation





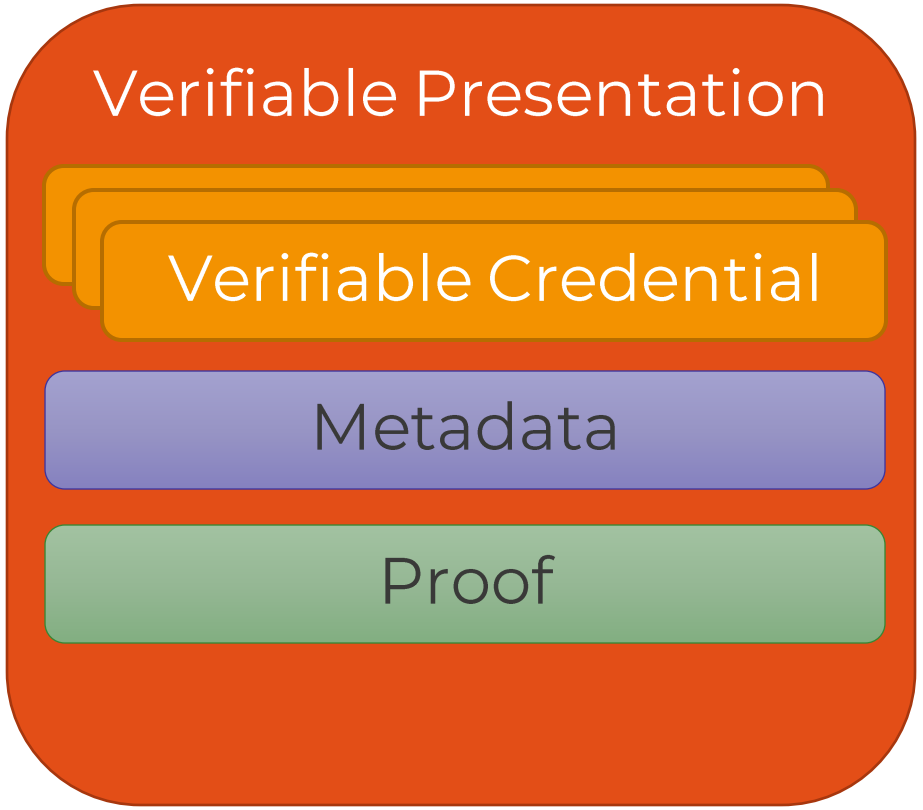
condatis
a sitekit company

Verifiable Presentation



Verifiable Presentation

```
{
    "@context": [ "https://www.w3.org/2018/credentials/v1" ],
    "id": "urn:uuid:00000000-0000-0000-0000-000000000001",
    "type": [ "VerifiablePresentation" ],
    "holder": "did:example:abc123",
    "verifiableCredential": [
        {
            "id": "http://condatis.com/credentials/987",
            "type": [ "VerifiableCredential" ],
            "credentialSubject": {
                "worksAt": "Condatis"
            } ,
            "proof": { ... }
        }
    ],
    "proof": {
        "type": "RsaSignature2018",
        "created": "2020-11-18T12:30:00Z",
        "proofPurpose": "authentication",
        "verificationMethod": "did:example:abc123#keys-1",
        "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
        "domain": "4jt78h47fh47",
        "jws": "ey..."
    }
}
```

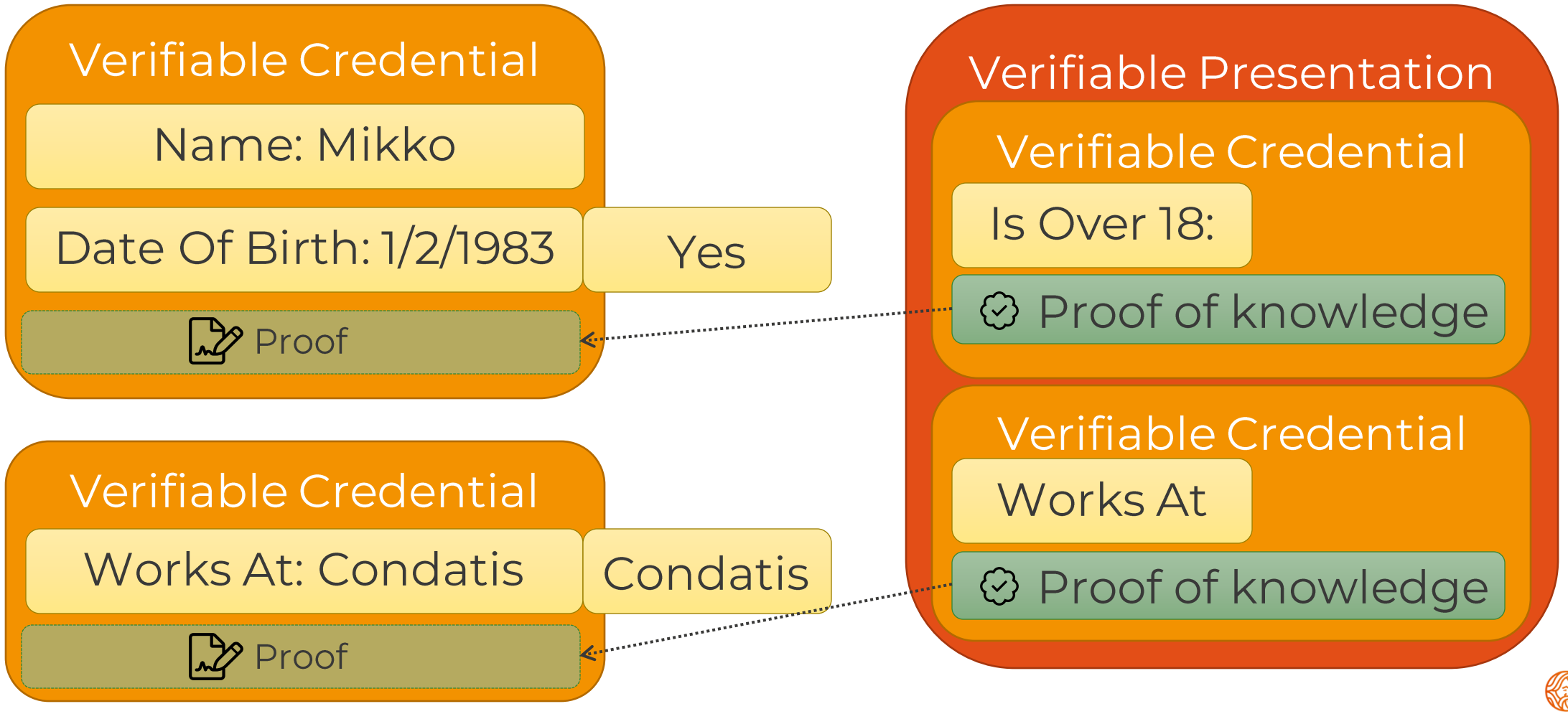


condatis
a sitekit company

Zero Knowledge Proofs (ZKP)

- Produce derived claims and credentials
- Combine multiple credentials into presentation
- Selectively disclose claims
- Prevent identifying underlying credential

Zero Knowledge Proofs (ZKP)



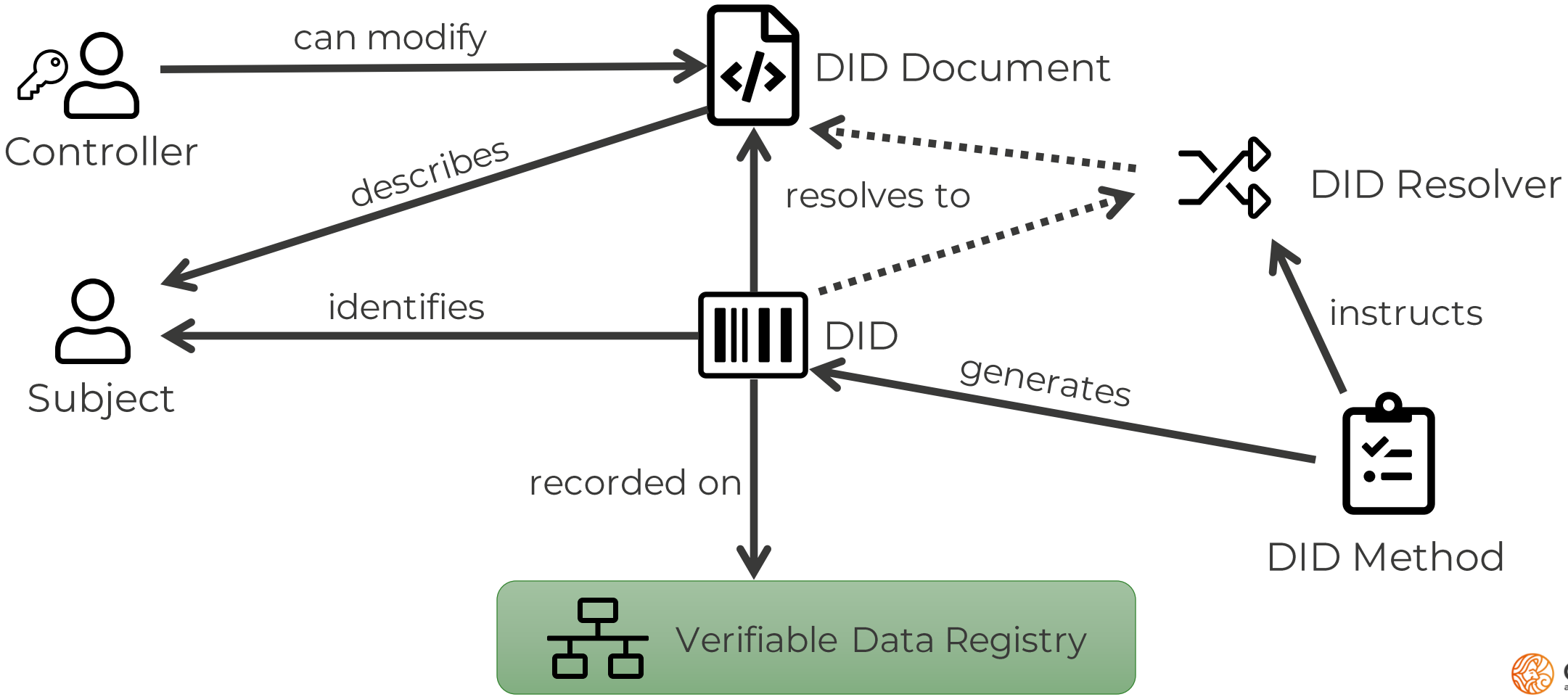
condatis
a sitekit company

condatis
a sitekit company

DID's and DID Documents

Overarching standards for Decentralized Identity

Decentralized Identifiers (DIDs)



condatis
a sitekit company

DID syntax

DID = DID Scheme | DID Method | Method-specific ID

```
did:sov:GUtCQ8jALUHB63A3dDyo8n
```

DID URL = DID | Path | Query | Fragment

```
did:sov:GUtCQ8jALUHB63A3dDyo8n/verify?q=key#key-1
```

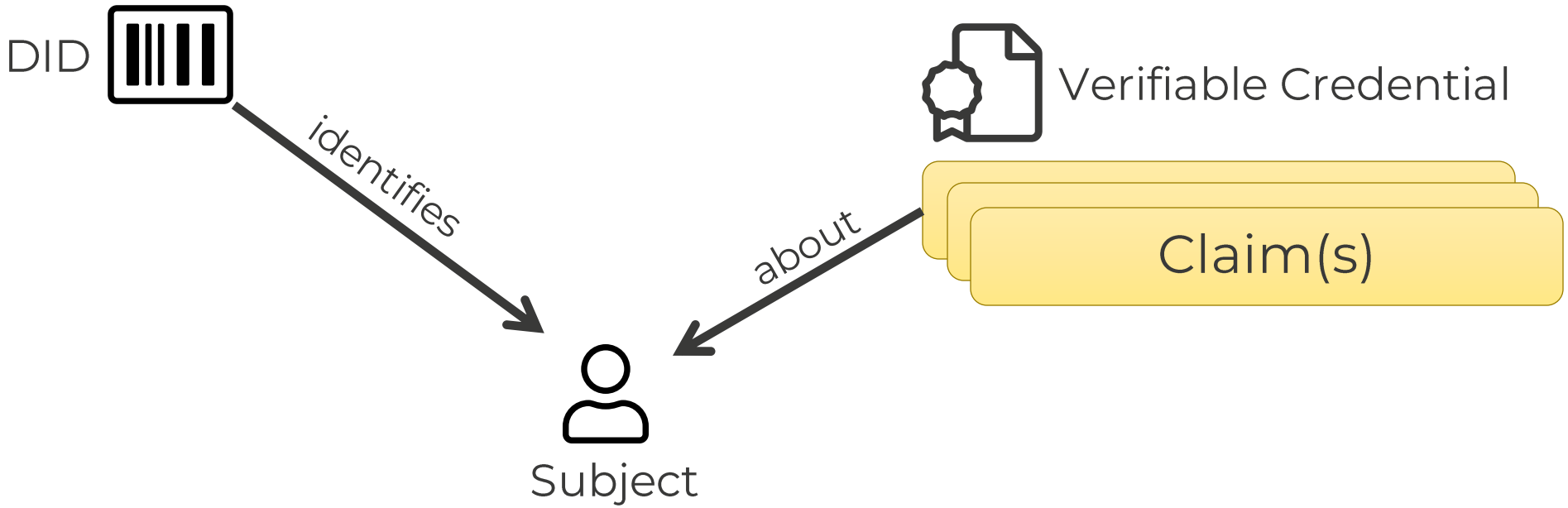
condatis
a sitekit company

DID Documents

```
{
    "id": "did:sov:GUtCQ8jALUHB63A3dDyo8n",
    "controller": "did:sov:GUtCQ8jALUHB63A3dDyo8n",
    "verificationMethod": [
        {
            "type": "Ed25519VerificationKey2018",
            "id": "did:sov:GUtCQ8jALUHB63A3dDyo8n#key-1",
            "publicKeyBase58": "9SNqr7AMEuXSn2RuwP8KUqq…"
        }
    ],
    "service": [
        {
            "id": "did:sov:GUtCQ8jALUHB63A3dDyo8n#agent",
            "type": "AgentService",
            "serviceEndpoint": "https://condatis.com/agent"
        }
    ]
}
```

condatis
a sitekit company

VC and DID Summary



condatis
a sitekit company

Protocols

Hyperledger Aries

- How to communicate?

  → DID Communication (DIDComm)

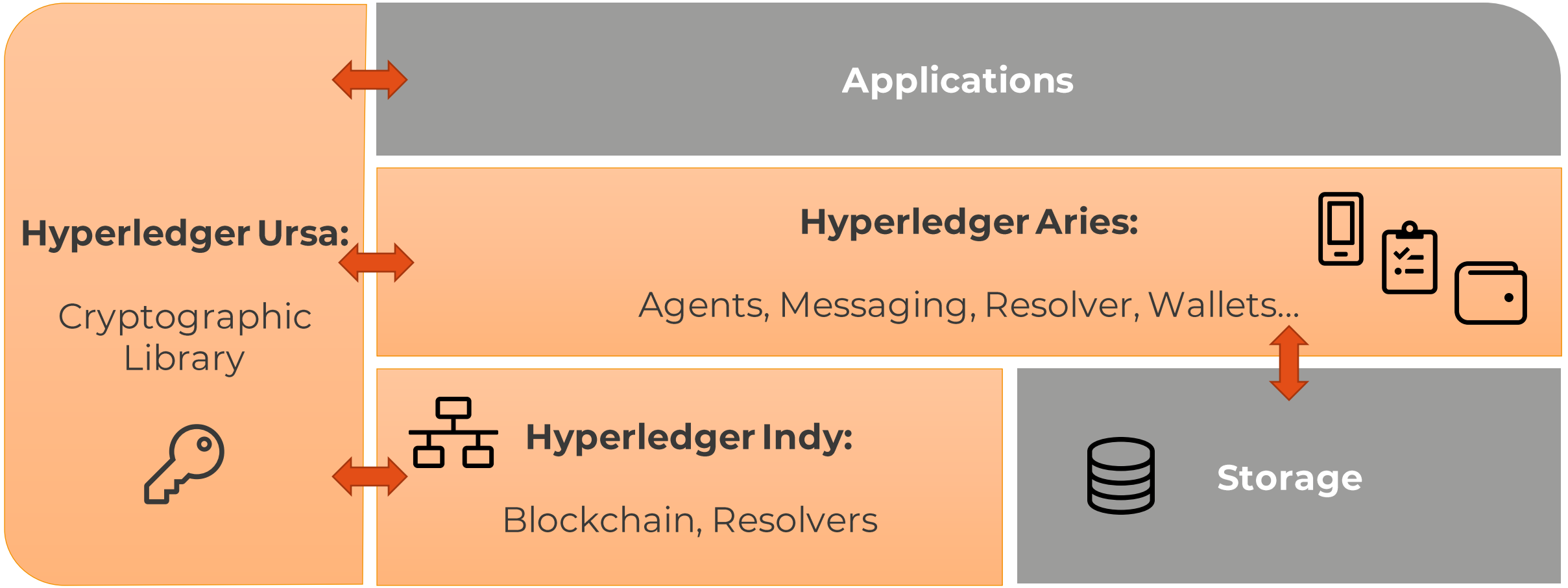
- How a Credential is issued from Issuer to Holder?

  → Issue Credential Protocol

- How to ask for Presentation from Holder?

  → Present Proof Protocol

Hyperledger Aries



condatis
a sitekit company

SIOP

SIOP

- How to communicate?

  → OIDC, SIOP, DID-SIOP

- How a Credential is issued from Issuer to Holder?

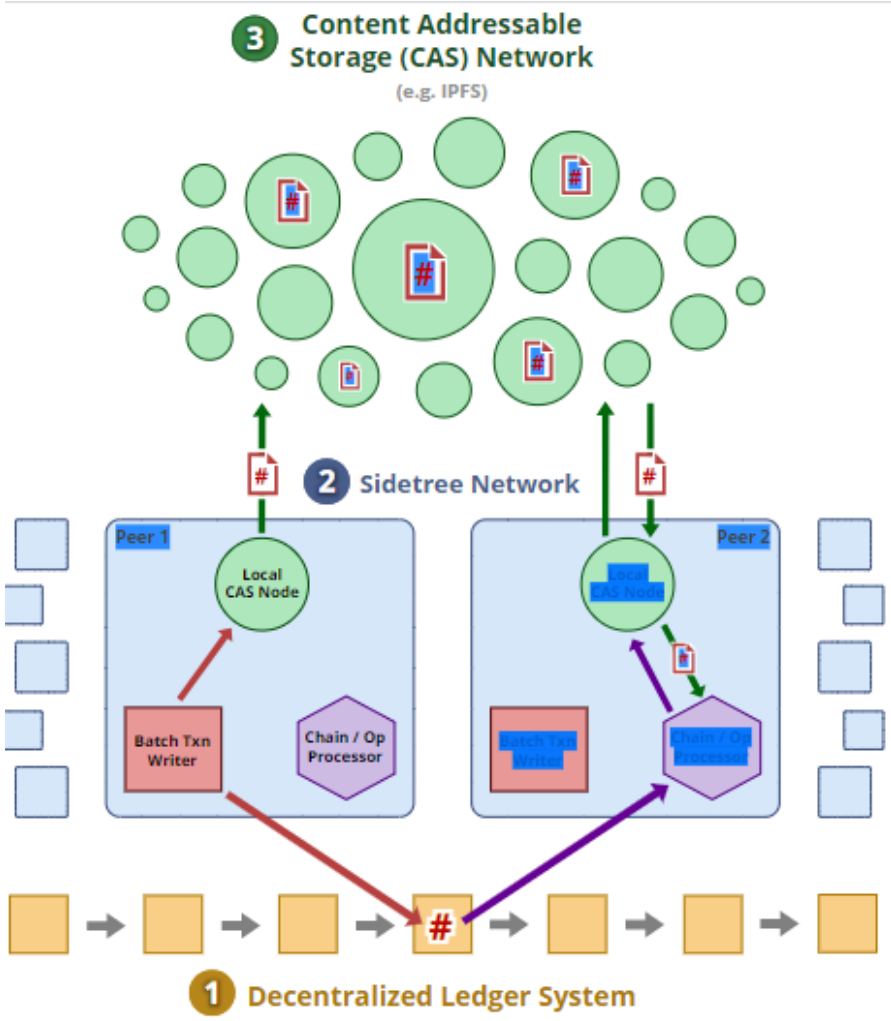
  → Issue Credential

- How to ask for Presentation from Holder?

  → Present Proof

SIOP

- ION
  - public, permissionless, decentralized DID overlay network
- Sidetree
  - Blockchain-agnostic protocol
- Bitcoin
  - decentralized ledger



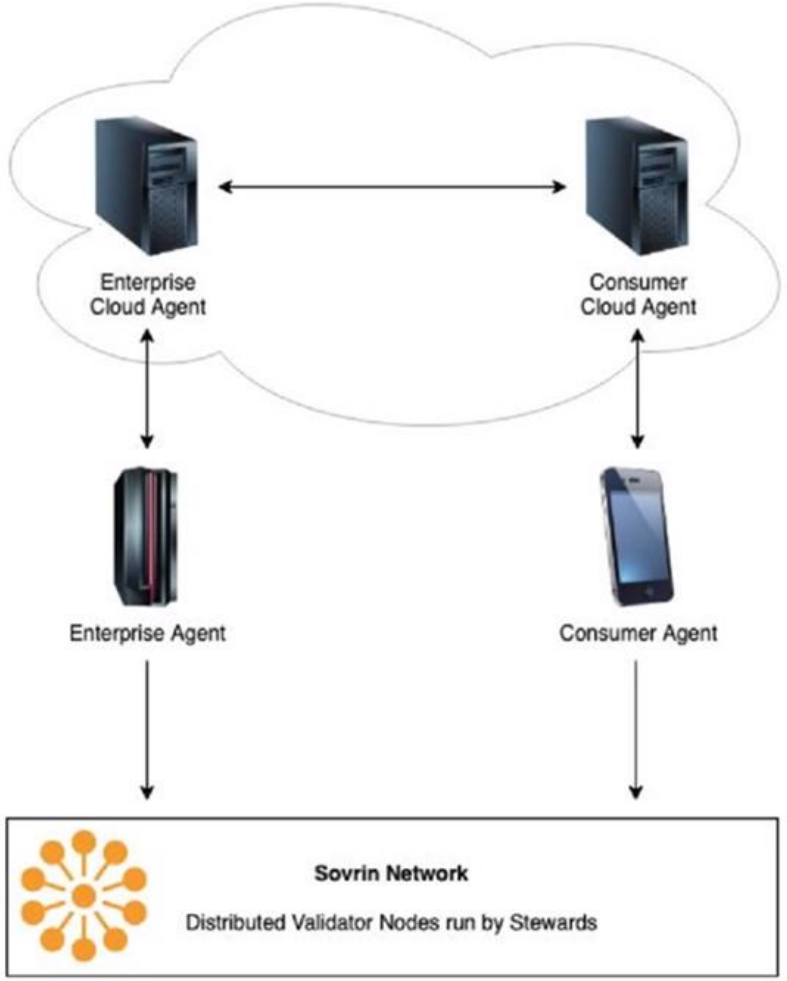
condatis
a sitekit company

condatis
a sitekit company

Agent and Wallets

Agents and Wallets

- Wallets
  - Connect.me
  - Trinsic
  - Microsoft Authenticator
- Agent types
  - Enterprise
  - Cloud
  - Consumer
  - Mediator



condatis
a sitekit company

condatis
a sitekit company

Interoperability

Interoperability?

- Interoperability challenges
  - Issuing and requesting proofs
  - Choice of Wallets
  - Different Agents needed
  - Support different protocols
    - Proof mechanisms, cryptography, messaging, ledgers

Interoperability?

- Presentation Exchange
  - Issuing and requesting proofs
  - https://identity.foundation/presentation-exchange/
- QR code or deeplink
  - openid:// or didcomm:// or wallet-specific handshake protocol

Condatis Interoperability approach

- Condatis SSI Middleware as abstraction layer
  - Evernym, Microsoft, Web wallets...
- Condatis Staff Passport Credential Issuer and Verifier Client
- Condatis Credential Verifier App
- OIDC Bridge to allow Relying parties to consume verified credentials as claims
  - Configurable, Customizable

condatis
a sitekit company

condatis
a sitekit company

Demo

condatis
a sitekit company

Summary

Summary

- Standards
- Protocols
- Agents and Wallets
- Interoperability
- Condatis Decentralised Identity Staff Passport

condatis
a sitekit company

condatis
a sitekit company

Questions

Upcoming webinars

SSI webinar series

	Title
December	Aries Hyperledger

Condatis Youtube Channel

Upcoming B2C webinars

	Title
December	Federation and Single Sign-On for Azure AD B2C
January	API integration and user migration using Azure AD B2C

condatis
a sitekit company

condatis
a sitekit company

Thank you for joining us!

Are you interested in using our decentralised identity solution. Let's talk! Drop us a line on **info@condatis.com**, and we'll get you set up with a specialist.