TrustBuilder

enhansa

docbyte

athumi
het Vlaams Datanutsbedrijf

randstad

Data Minimization in a Solid network

Paul Henon, Docbyte
Ben De Meester, IDLab

24/2/2025

IDLab
INTERNET & DATA LAB

imec-mict-ugent

Challenge: Privacy in an increasingly Public World

- Situation
  - information is everywhere
  - retaining control is hard
  - privacy expectations and legislation are demanding
  - reliability of information is often in question
  - secure information exchange is fragmented and non-standardised
- And yet
  - the need for information exchange is very real
  - individuals and companies crave trustworthy information
  - security and reliability are increasingly important
- But
  - individuals don't want to share everything with anyone
  - individuals want to have control over their information

Solution: Data Minimisation

- Concept
  - Reduce the full data set to just the elements the requester needs
  - Derive required information from full data
  - Maintain evidentiary value

- Example
  - Recruiter requires
    - at least 30yo
    - master's degree
  - Personal data contains
    - date of birth
    - full master's diploma details
  - Minimisation will
    - derive age from DOB
    - reduce diploma to just the master's title
    - maintain evidence provided by the authentic source

Research

How to do data minimization in a Solid network?

Requirements
- Accredited data
- Data minimization method
- Decentralized network
  - Original data issuer
  - Original and minimized data holder
  - Minimized data verifier
  - Data minimisation service

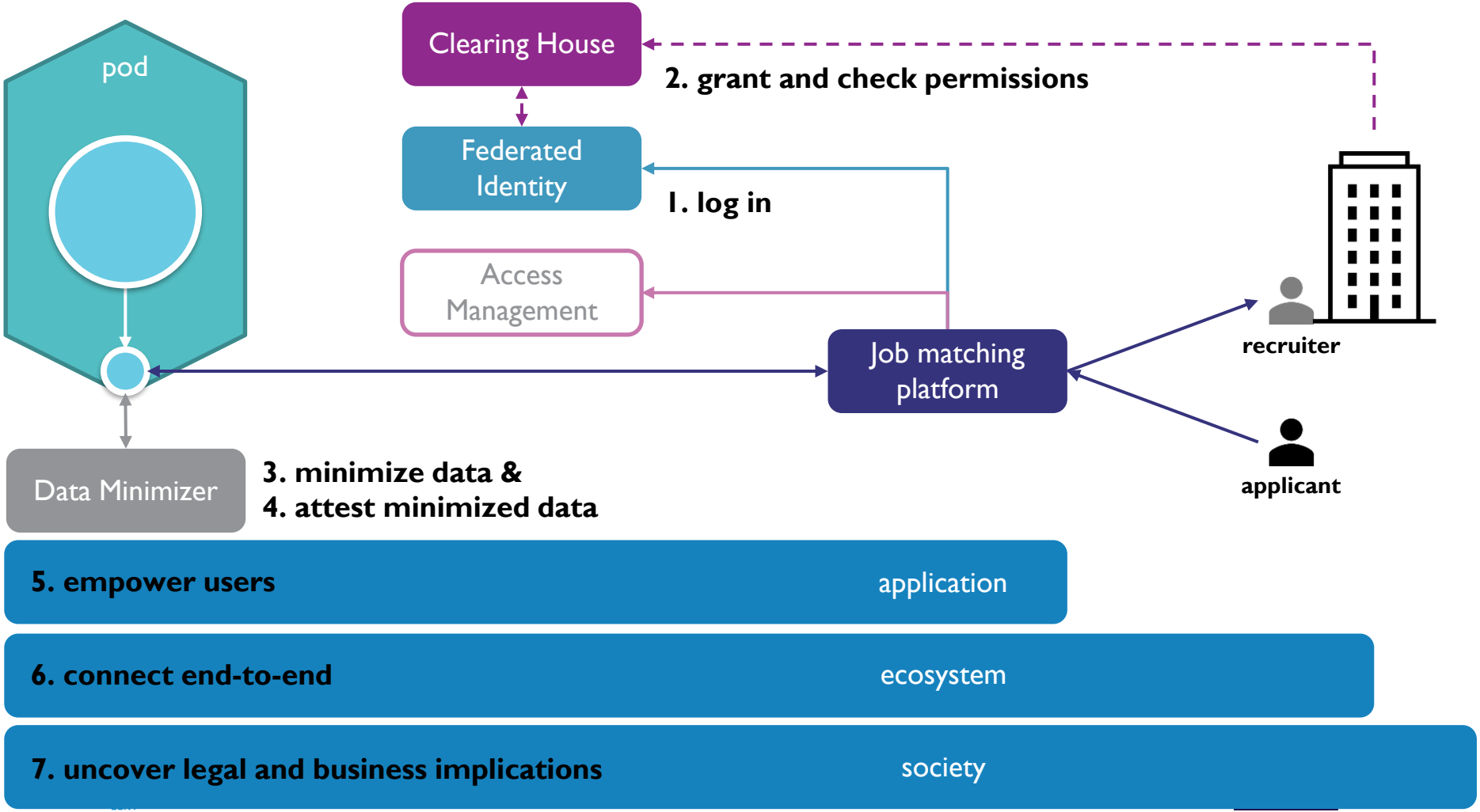
Mind for interoperability

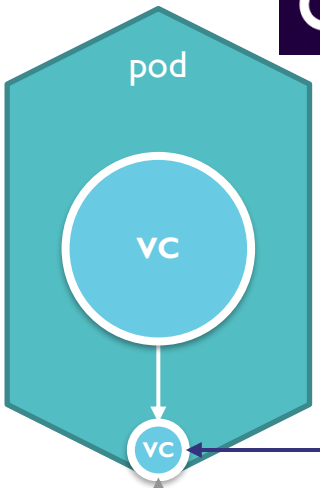
Research

How to do data minimization in a Solid network?

Requirements

Accredited data	diploma data
Data minimization method	selective disclosure, predicate proofs, range queries
Decentralized network	
Original data issuer	Flemish Government via Athumi
Original and minimized data holder	Citizen (that's you!)
Minimized data verifier	Recruiter from Randstad
Data minimisation service	DocByte


pod
Clearing House
2. grant and check permissions
Federated Identity
1. log in
Access Management
Job matching platform
recruiter
applicant
Data Minimizer
3. minimize data &
4. attest minimized data
5. empower users
application
6. connect end-to-end
ecosystem
7. uncover legal and business implications
society



Data Minimizer

3. minimize data &
4. attest minimized data

Job matching platform

recruiter

applicant

Solution

Accredited data via Verifiable Credentials (VCs)

Mind that how the VC gets into the pod is out of scope

related work is, e.g., OIDC4VP and DIDComm

Minimization by deriving a new VC

using methods such as selective disclosure and range query proofs

Result is a minimized VC that can be verified using the original signature,

i.e. no need for re-accreditation by third party

Verifiable Credential

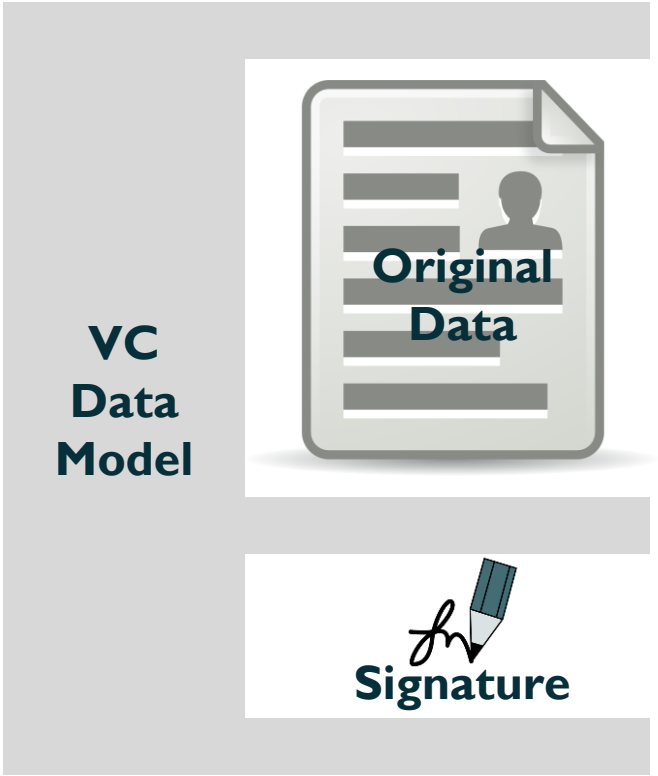
A data model that specifies **how to represent a signed piece of data**

i.e., if the data changes, the signature no longer matches

using an extensible set of Digital Signature Algorithms

each with different characteristics and functionalities

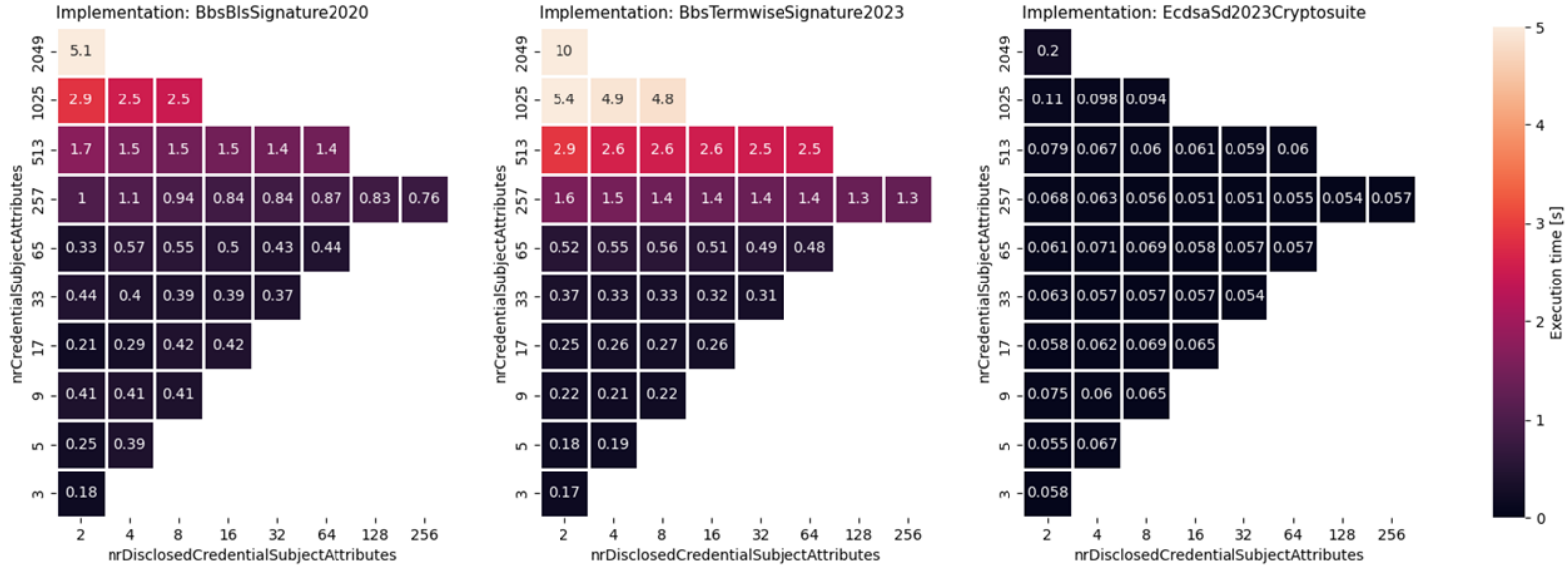
W3C Recommendation of VC v2.0 is close to completion



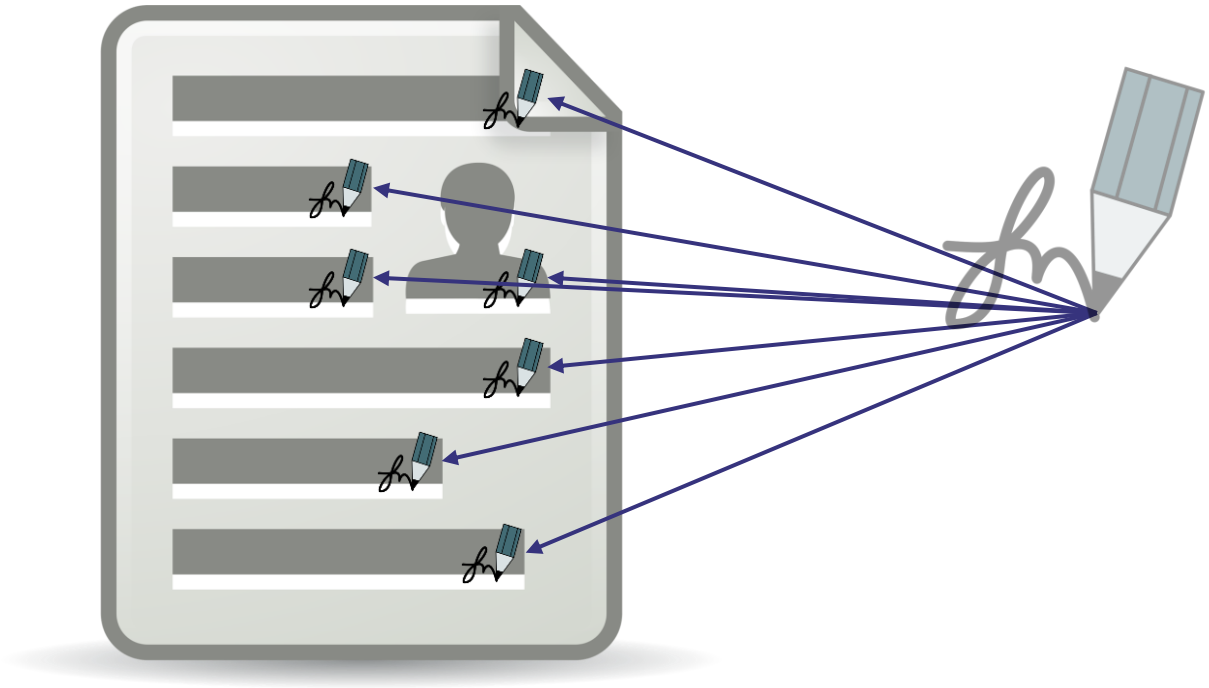
Different Digital Signature Algorithms have different characteristics

	Cryptosuite			
Characteristic	**ECDSA**	**EdDSA**	**BBS+ (2020)**	**BBS Termwise (2023)**
Curve type	Weierstrass Eliptic Cryptographic Curve (ECC)	Twisted Edwards	Bilinear Pairing-based	Bilinear Pairing-based
Curve used	P-256	Edwards25519 (related to Curve25519)	BLS12-381	BLS12-381
Implementation used	DigitalBazaar ecdsa-sd-2023-cryptosuite v3.4.1	DigitalBazaar ed25519-signature-2020 v5.4.0	MATTR jsonld-signatures-bbs v1.2.0	ZKP-LD jsonld-proofs v0.14.0
NIST approved	✓ (FIPS 186-2, 2000)	✓ (FIPS 186-5, 2023)	✗	✗
Features	Sign/Verify - Selective Disclosure (JSONPath Pointer)	Sign/Verify	Sign/Verify Unlinkability Selective Disclosure (JSON-LD Frame)	Sign/Verify Unlinkability Selective Disclosure (JSON-LD Frame) Range Queries (JSON-LD Frame)
Adoption	Widely adopted (TLS), specifically in cryptocurrency (Blockchain)	High (SSH, TLS, secure messaging)	Emerging in privacy-preserving identity systems (Verifiable Credentials, SSI)	Emerging in privacy-preserving identity systems (Verifiable Credentials, SSI)

Different Digital Signature Algorithms have different characteristics



Selective Disclosure due to Bilinear Pairing-based algorithm



Range proofs (on top of selective disclosure)


```
{ "@context": [ "https://www.w3.org/2018/credentials/v1", "https://www.w3.org/ns/data-integrity/v1", "https://zkp-ld.org/context
  "type": "VerifiablePresentation",
  "proof": {
    "type": "DataIntegrityProof", "created": "2024-06-12T09:21:12.633Z", "challenge": "abc123", "cryptosuite": "bbs-termwise-pro
    "proofValue": "uomFhWQPjAgAAAAAAAAAAgy6M8oil8niZJq6DbWmAy-hDIVwoIGa63OzL086ulKOpFjoHRmACTwG9lor5KIIutH0F0Gxv16CC[...] AwQFBg
  },
  "verifiableCredential": {
    "id": "http://example.org/credentials/1/1", "type": "VerifiableCredential",
    "proof": { "type": "DataIntegrityProof", "created": "2023-01-01T00:00:00Z", "cryptosuite": "bbs-termwise-signature-2023", "p
    "credentialSubject": {
      "id": "did:example:john", "type": "http://schema.org/Person",
      "http://schema.org/birthDate": {}, #selective disclosure
      "http://schema.org/familyName": "Smith", "http://schema.org/givenName": "John",
      "http://schema.org/homeLocation": {
        "id": "did:example:cityA",
        "http://schema.org/maximumAttendeeCapacity": {
          "id": "_:b4“ #range verification
        } } },
    "expirationDate": "2026-01-01T00:00:00Z", "issuanceDate": "2023-01-01T00:00:00Z", "issuer": "did:example:issuer0"
  },
  "predicate": {
    "type": "Predicate", "circuit": "circ:lessThanPrvPub",
    "private": [ { "type": "PrivateVariable", "val": "_:b4",                                    "var": "lesser“ } ],
    "public": [  { "type": "PublicVariable",  "val": { "type": "xsd:integer", "@value": "50000“ }, "var": "greater“ } ] } }
```

Implementation

Verifiable Credentials API v0.3

An HTTP API for Verifiable Credentials lifecycle management

Draft Community Group Report 18 February 2025

Latest published version:
https://www.w3.org/vc-api/

Latest editor's draft:
https://w3c-ccg.github.io/vc-api/

Editor:
TBD

Feedback:
GitHub w3c-ccg/vc-api (pull requests, new issue, open issues)
public-credentials@w3.org with subject line `[vc-api] … message topic …` (archives)

Abstract

Verifiable credentials provide a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable. This specification provides data model and HTTP protocols to issue, verify, present, and manage data used in such an ecosystem.

Results

Selective disclosure in demonstrator

i.e., we can share our diploma degree without sharing our full diploma

Limitations

Range query proofs are in proof-of-concept, not in demonstrator

We had to create new VCs for Athumi (so re-signing),
as different VC versions have different functionalities

This resigning should not be needed: focus for future work

3 publications (1 accepted, 2 submitted)

VC exchange protocol (accepted)

Application of selective disclosure for pseudonimity (submitted)

Comparison of digital signature algorithm characteristics (submitted)

Docbyte's Role in the Process

- Data processor for Athumi who is hosting the Solid pods
  - Docbyte minimisation called as a function from within Athumi's platform
  - Providing minimised VC's
  - Maintaining accreditation status
  - Supporting revocation status updates

- Investigation of deployment options
  - Default Docbyte platform is AWS based
  - Initial deployment as VM → works perfectly
  - Second scenario container-based → equally successful
  - Third scenario as Lambda service (serverless) → ideal scenario for maintainability

Docbyte's Outlook: What can we do with it?

- **Docbyte Vault** = Docbyte's core activity = digital archiving
  - qualified (eIDAS compliant) and non-qualified
  - living archive = information retrieved every day
  - serving as an authentic source of information
  - maintaining evidence across time
  - providing ingest and dissemination functions

- Future options under consideration
  - VC's are an interesting means to share information
  - Minimisation functions have more potential than the HR case
  - Solid pods as a user-controlled carrier of information offer potential in a personalised archiving context

- Conclusion: useful research results with real options for future implementation in Docbyte solutions

TrustBuilder

enhansa

docbyte

athumi
het Vlaams Datanutsbedrijf

randstad

Data Minimization in a Solid network

Paul Henon, Docbyte
Ben De Meester, IDLab

24/2/2025

IDLab
INTERNET & DATA LAB

imec-mict-ugent

embracing a better life