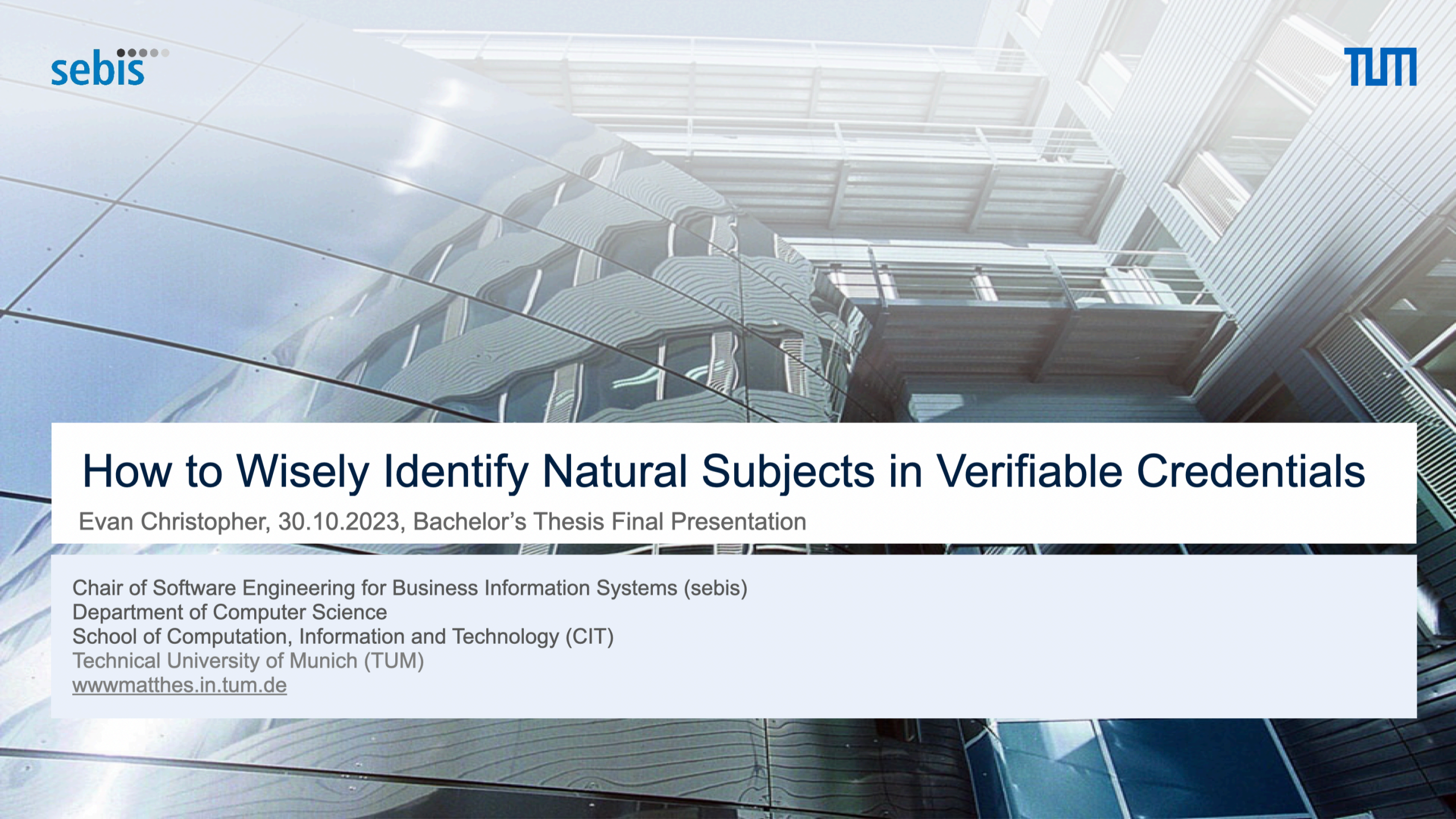


How to Wisely Identify Natural Subjects in Verifiable Credentials

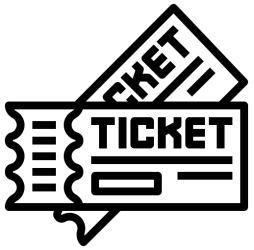
Evan Christopher, 30.10.2023, Bachelor's Thesis Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

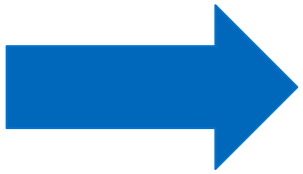
Outline

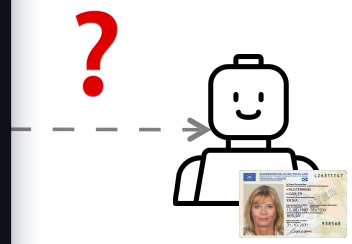
1. Motivation
2. Research Questions
3. Literature Survey
4. Implementation
5. Demo
6. Limitations and Future Work
7. Summary

Motivation – Credentials



Physical Credentials





Verifiable Credentials (digital)

Research Questions

RQ1 What are the existing solutions and proposals for including identifying information in VCs?

A. How are identifying information included in VCs from these existing solutions?

B. How do the existing approaches compare?

RQ2 How can updates to identifying information be handled in VCs?

Literature survey, Taxonomy

RQ3 How can we engineer effective identity credentials within the GX-Credentials project?

A. Should the existing schema be revised, and which identity attributes need to be included?

B. How can the GX-Credentials project be extended to facilitate the revised identity credential?

Design/ implement

RQ1: Methodology

What are the existing solutions and proposals for including identifying information in VCs?

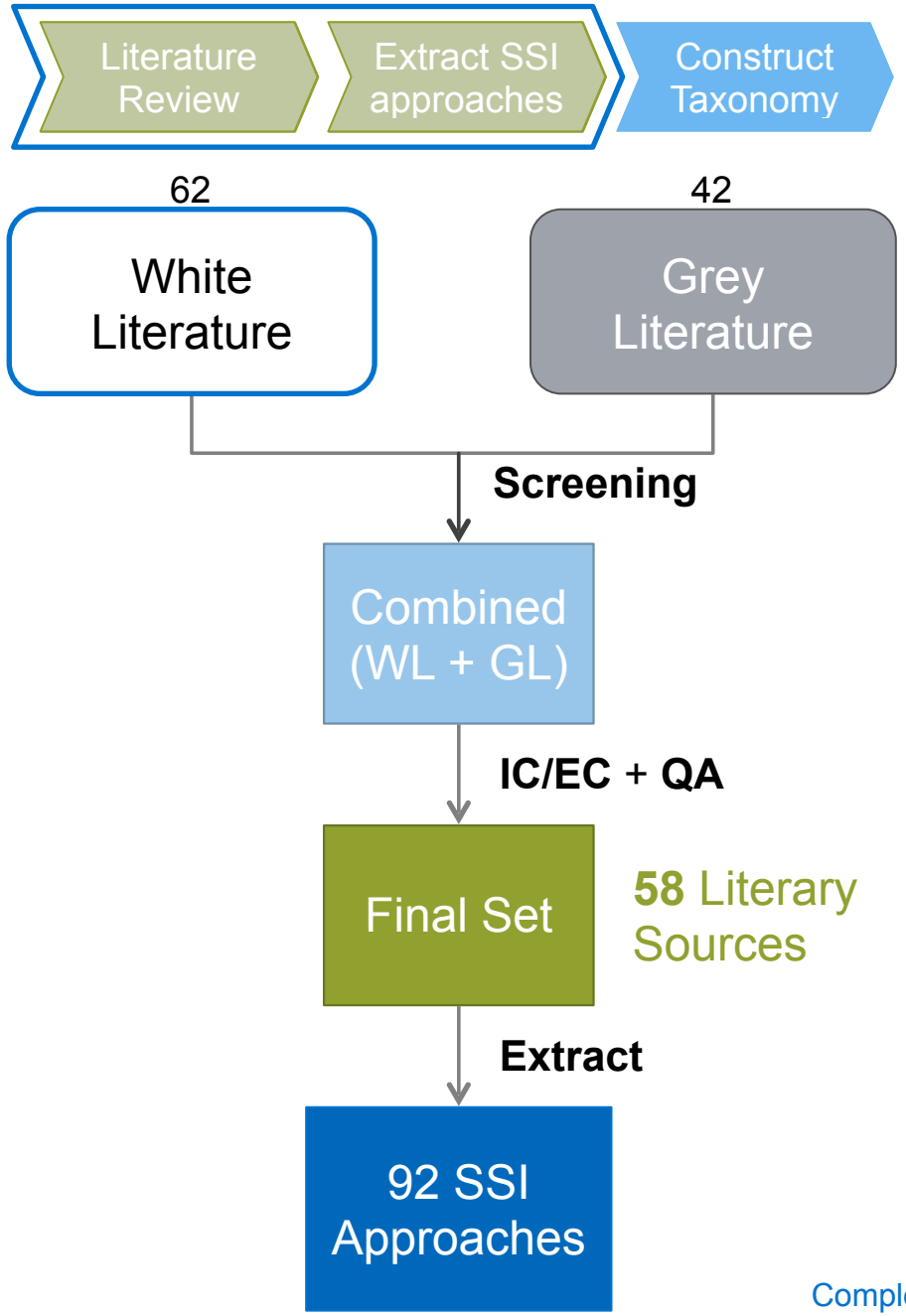
1. **(Adapted) Multivocal Literature Review (MLR)** [1]
   - Find existing approaches from white and grey literature (blogs, documentation, etc.)
   - Used for planning – data extraction
2. **Nickerson et al.** [2]
   - Create a taxonomy to differentiate existing approaches

[1] Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and software technology, 106, 101-121.

[2] Nickerson, R., Varshney, U. & Muntermann, J. A method for taxonomy development and its application in information systems. Eur J Inf Syst 22, 336–359 (2013). https://doi.org/10.1057/ejis.2012.26

RQ1: Methodology – Literature Review

- **Keywords**
  - Self-sovereign Identity (SSI), identity management, natural person, legal person, person, verifiable credentials
- **Databases**
  - IEEE, ACM, Scopus, Google Scholar, Google Search
- **Inclusion Criteria (IC)**
  - **IC-1** Papers that include natural subjects in VCs.
  - **IC-2** Papers that are accessible through institutional login.
- **Exclusion Criteria (EC)**
  - **EC-1** Papers without sufficient technical details or processes.
  - **EC-2** Papers that focus on domains that do not involve natural subjects.
  - **EC-3*** Survey papers.
- **Quality Assessment Table** used as IC/EC for Grey Literature
- Documented in a Notion database

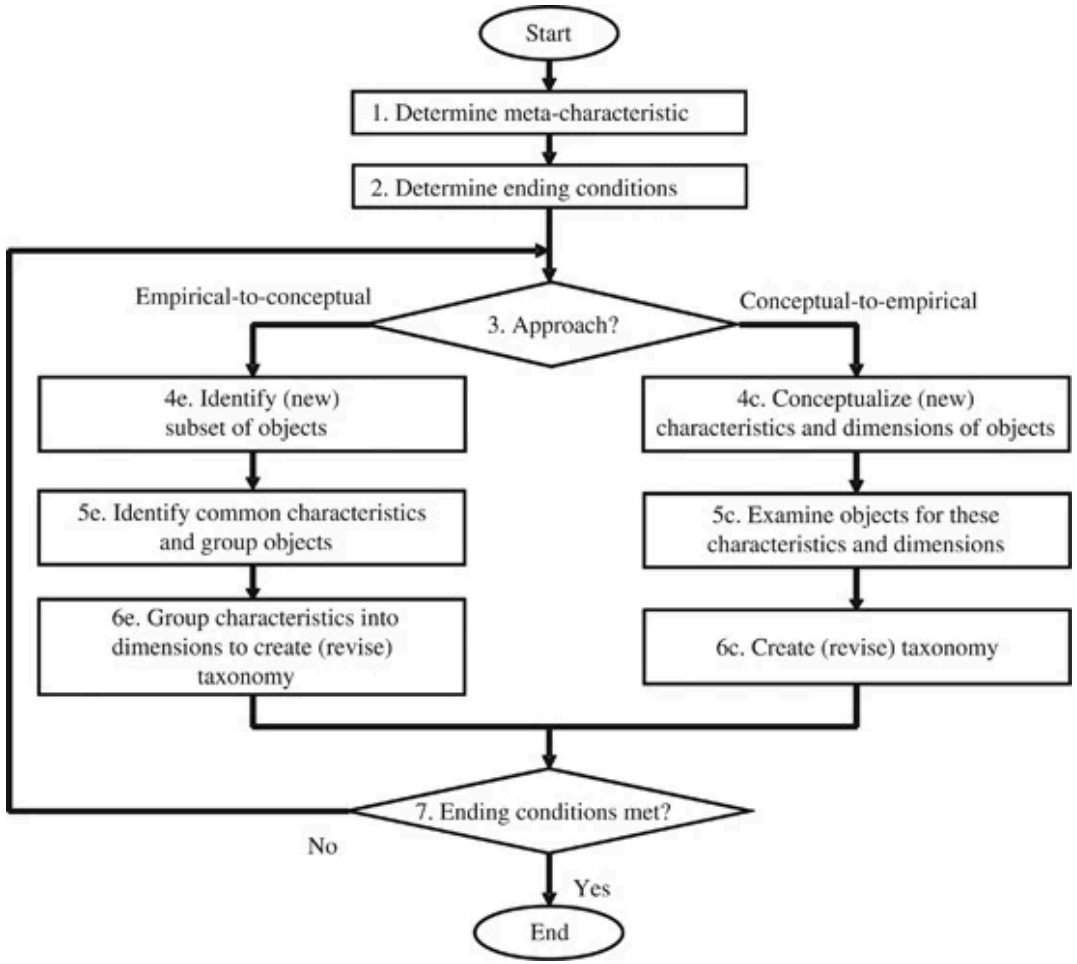


Complete LR Process

* Consider surveys found in WL as GL

RQ1: Methodology – Taxonomy Construction

Literature Review → Extract SSI approaches → **Construct Taxonomy**



- **Iterative process**
  - End? When *Ending Conditions* (objective and subjective) are fulfilled
- **Approaches**
  - Conceptual and Empirical
- **Meta-characteristic**
  - Most comprehensive characteristic of all potential characteristics in the taxonomy

Chosen Meta-Characteristic:
Characteristics of user identification approaches in SSI such as how the user's PII is included, the data flow, formats, identity verification, management, and storage location.

- **Objects of Interest**
  - **Initial** pool of **92** approaches → Final set: **35** approaches
  - Removed solutions that are:
    - not end-user (natural subject) identification
    - not using VCs
    - non-SSI
    - incomplete/deprecated

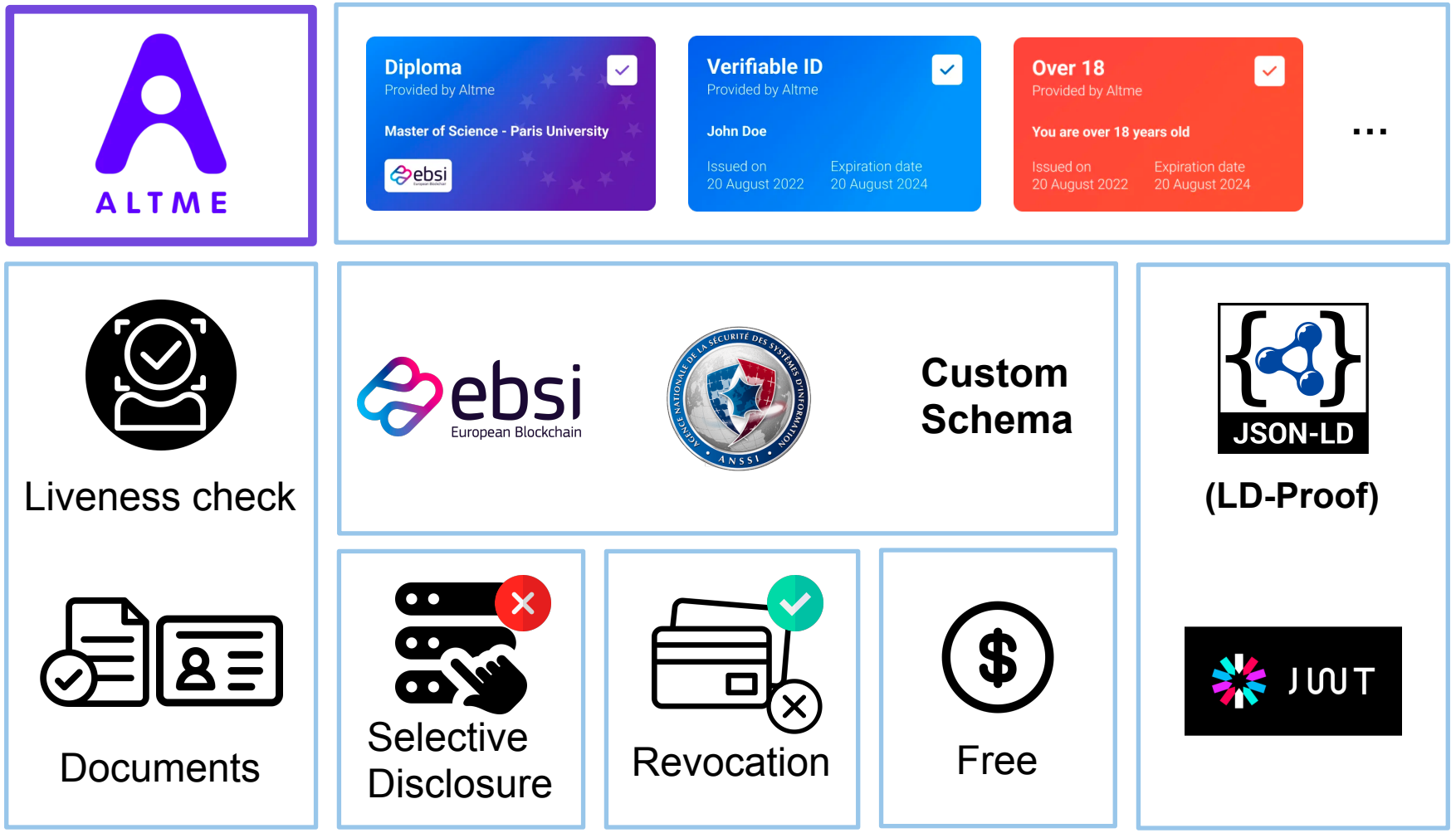
RQ1: Proposed Taxonomy

Dimensions	Characteristics						E/N*
PII Location	Standalone			Bundled			E
PII Type	Natural			Alternative			N
Identification Data Source	Gov-ID	Non-Gov-ID	Biometrics	PoP	None	Unspecified	N
Identification Authority	End-user-asserted	Third-party-asserted	SSI-Integrator-asserted		First-party-asserted		N
Projected Cost Per User	Free	Per-issuance + operation		Recurring base fee		Unspecified	N
VC Format	LDP-VC		JWT-VC		Unspecified		N
Schema Standard	Standardized			Flexible			N
Selective Disclosure	Yes			No			E
Credential Revocation	Yes		No		Unspecified		E

* Exclusivity of the dimension. E = exclusive, N = non-exclusive characteristics

Complete Taxonomy Assignment

RQ1: Proposed Taxonomy – Example of an SSI Approach: Altme



RQ1: Proposed Taxonomy – Example Assignment

Dimensions	Characteristics						E/N*
PII Location	Standalone			Bundled			E
PII Type	Natural			Alternative			N
Identification Data Source	Gov-ID	Non-Gov-ID	Biometrics	PoP	None	Unspecified	N
Identification Authority	End-user-asserted	Third-party-asserted	SSI-Integrator-asserted		First-party-asserted		N
Projected Cost Per User	Free	Per-issuance + operation		Recurring base fee	Unspecified		N
VC Format	LDP-VC		JWT-VC		Unspecified		N
Schema Standard	Standardized			Flexible			N
Selective Disclosure	Yes			No			E
Credential Revocation	Yes		No		Unspecified		E

*Assigned Characteristics

* Exclusivity of the dimension. E = exclusive, N = non-exclusive characteristics

Complete Taxonomy Assignment

RQ1: Proposed Taxonomy – Discussion on Characteristics

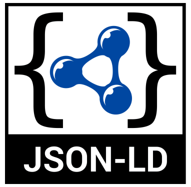
Complete Taxonomy Assignment

Table 5.3.: Proposed Taxonomy of SSI Approaches

Non-exclusive/ Exclusive	E		N		N						N				N				N			N		E		E		
SSI approaches	PII Location		PII Type		Identification Data Source						Identification Authority				Projected Cost per User				VC Format			Schema Standard		Selective Disclosure		Credential Revocation		
	Standalone	Bundled	Natural	Alternative	Gov-ID	Non-Gov-ID	Biometrics	PoP	None	Unspecified	End-user-asserted	Third-party asserted	SSI-Integrator asserted	First-party asserted	Free	Per-issuance + operation	Recurring base fee	Unspecified	LDP-VC	JWT-VC	Unspecified	Standardised	Flexible	Yes	No	Yes	No	Unspecified
Civic	x		x	x	x	x	x	x				x	x			x	x		x	x			x	x		x		
Jolocom		x	x	x						x	x				x						x		x	x		x		
Midy (Evernym)	x		x		x		x					x			x						x		x		x			x
Soltani et al. [112]	x		x	x	x									x		x					x		x		x	x		
MediLinker	x		x	x	x	x								x				x			x		x		x	x		
Alastria ID	x		x		x	x							x			x	x		x			x		x		x		
Tahlil et al. [49]		x	x		x									x				x			x		x	x		x		
Blockcerts		x	x						x		x					x			x				x		x	x		
Cosmos Cash		x	x						x		x							x	x				x		x			x
Dock		x	x	x	x	x	x						x			x	x		x	x			x	x		x		
Saidi et al. [113]		x		x					x		x							x			x		x		x	x		
Herbkle et al. [114]		x	x	x		x								x				x	x			x			x			x
Hamer et al. [115]	x		x				x					x						x	x				x		x	x		
Stockburger et al. [116]	x		x	x	x									x	x						x		x	x			x	
Wang et al. [117]		x		x	x							x						x			x		x		x			x
WeIdentity		x		x	x									x				x	x				x	x		x		
Xu et al. [118]	x			x					x		x							x			x		x		x	x		
M. Morosi [119]		x	x		x									x				x	x				x	x		x		
C. Sehlke [26]	x		x		x	x								x	x				x			x			x	x		
Trinsic		x	x	x	x	x	x						x			x			x	x			x	x		x		
ValID		x	x	x					x		x				x						x		x		x	x		
Altme		x	x		x	x		x				x			x				x	x		x	x		x			x
Datakeeper	x		x		x	x	x						x			x	x		x				x	x		x		
Gataca.io		x	x	x	x	x	x	x					x			x	x		x	x		x	x	x		x		
GlobalID		x	x	x	x	x	x	x				x	x			x					x		x		x	x		
Indicio Proven		x	x	x	x	x	x	x					x			x					x		x	x		x		
Lissi		x	x	x	x	x							x			x	x				x		x	x		x		
Mattr		x	x	x	x	x	x						x				x		x			x	x	x		x		
Meeco		x	x	x					x				x				x			x			x	x			x	
Verida	x		x		x	x							x			x				x			x	x				x
VIDchain	x		x						x				x					x		x		x	x		x	x		
Walt.id	x		x	x					x				x					x	x			x	x		x	x		
Belchior et al. [120]		x	x						x					x	x						x		x	x		x		
Rahman et al. [121]	x		x		x									x				x			x		x	x				x
Satybaldy et al. [122]		x	x	x	x	x								x				x	x			x		x		x		

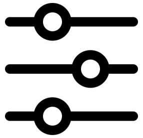
Identification Data Source

VC Format



(LD-Proof)

Schema Standard



Custom Schema

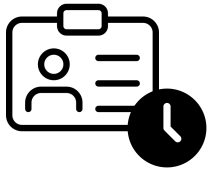
Selective Disclosure

Revocation

RQ2: Verifiable Credentials Update Mechanisms

How can updates to identifying information be handled in VCs?

Short-lived Credentials

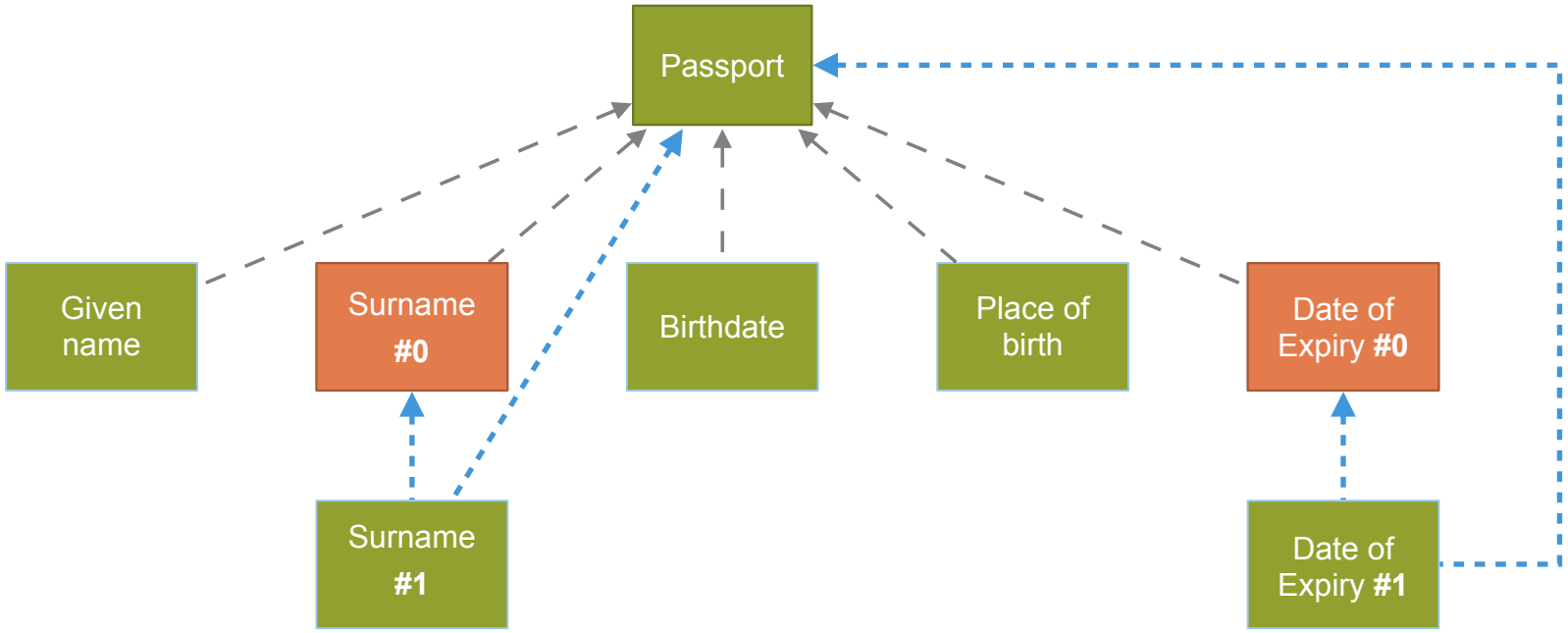


Validity period?

❌ Operational overhead

❌ Suboptimal UX

Atomic Credentials



✅ Granular control/policies

❌ Malformed credentials

❌ Hiding (negative) updates

RQ2: Verifiable Credentials Update Mechanisms

How can updates to identifying information be handled in VCs?

Credential Disputes

```
{
   "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
   ],
   "id": "http://example.com/credentials/123",
   "type": ["VerifiableCredential", "DisputeCredential"],
   "credentialSubject": {
      "id": "http://example.com/credentials/245",
      "currentStatus": "Disputed",
      "statusReason": {
       "@value": "Address is out of date",
       "@language": "en"
      },
},
   "issuer": "https://example.com/people#me",
   "issuanceDate": "2017-12-05T14:27:42Z",
   "proof": {...}
}
```

VC Refresh Service

```
{
 "@context": [
   ...
 ],
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "https://example.edu/issuers/14",
 "issuanceDate": "2010-01-01T19:23:24Z",
 "credentialSubject": {
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "degree": {
    "type": "BachelorDegree",
    "name": "Bachelor of Science and Arts"
   }
 },
 "refreshService": {
   "id": "https://example.edu/refresh/3732",
   "type": "ManualRefreshService2018"
 }
}
```

W3C® (draft) specifications ✅, but: **due for removal** 🚨

RQ2: Verifiable Credentials Update Mechanisms

How can updates to identifying information be handled in VCs?

Updates  **Revocation**

- 🚨 General lack of research
- 🚨 Due for removal from standards

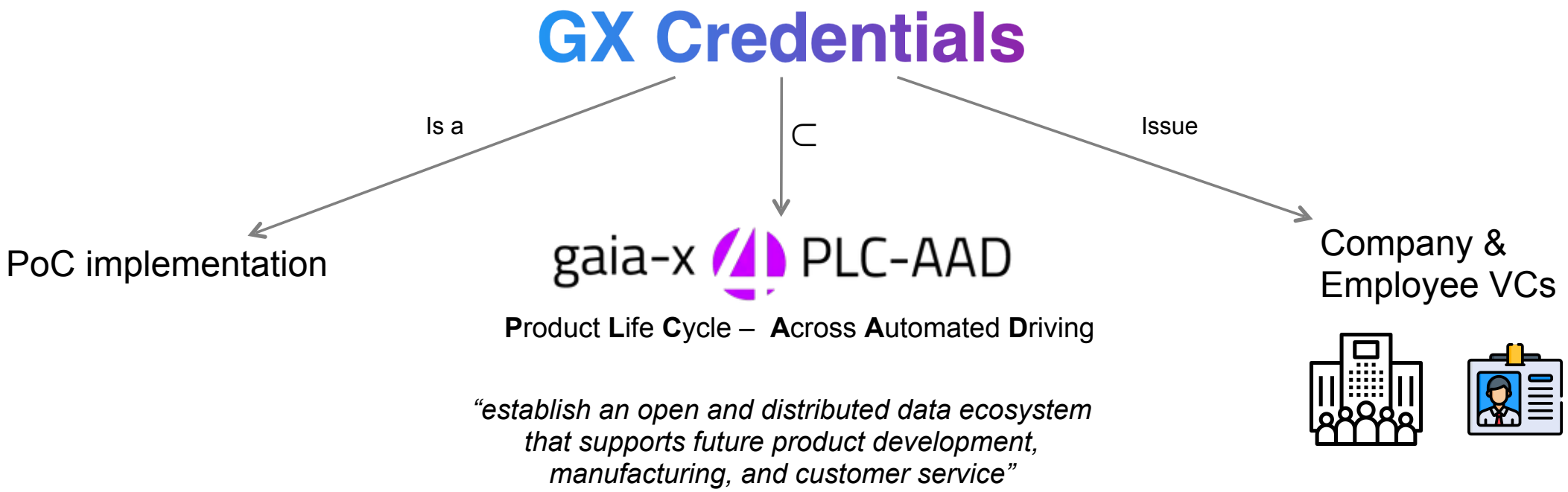
- ✅ Active research topic
- ✅ Support
- ❓ Scalability

VC Updates are not as important as we thought :(

Re-issuance is adequate!
… For now.

RQ3: Engineering Effective Identity Credentials – Context

How can we engineer effective identity credentials within the GX-Credentials project?



RQ3: Engineering Effective Identity Credentials

How can we engineer effective identity credentials within the GX-Credentials project?

GX Credentials

- ❌ ID binding
- ❌ VC schema for natural subjects
- ❌ **Selective Disclosure (SD)**

mandated by

Architecture **R**eference **F**ramework

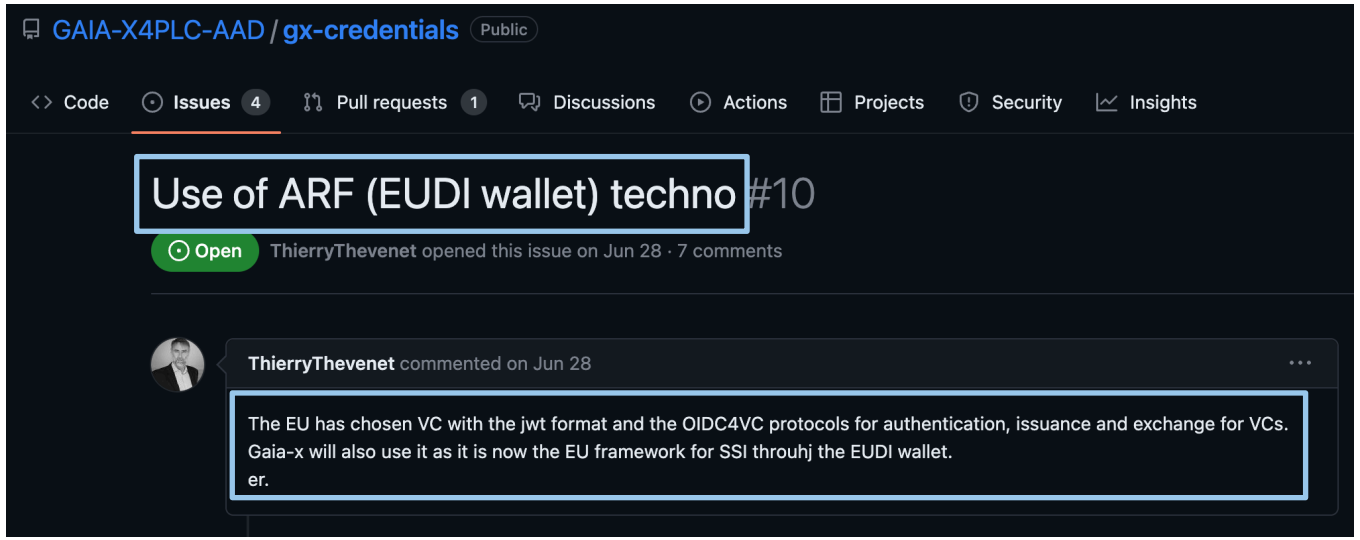
basis of

EUropean **D**igital **I**dentity

mandates

eIDAS

GDPR

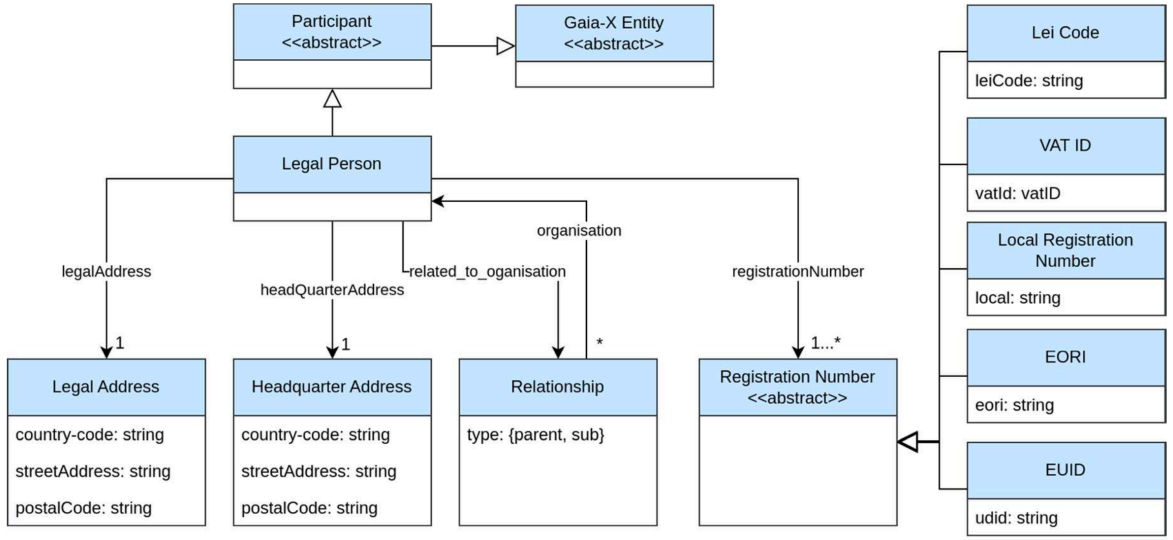


SD-JWT

- ✅ Simple
- ✅ Mature
- ✅ Post-quantum secure

RQ3: Engineering Effective Identity Credentials – Discussion

Gaia-X Participant Schema



eIDAS

ebsi European Blockchain

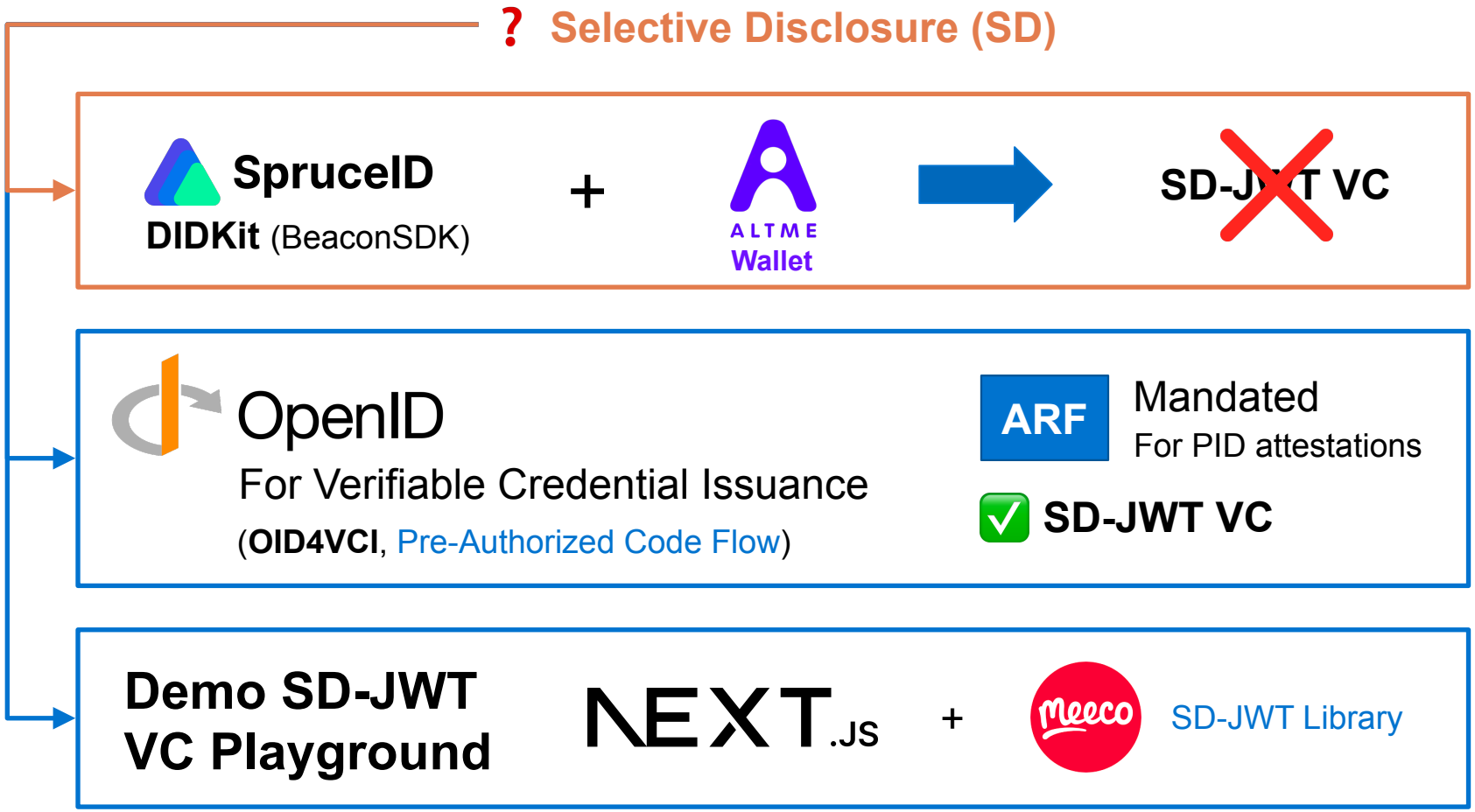
Proposed Employee Credential

	Attributes
Natural	Id
	familyName
	firstName
	dateOfBirth
	nationalIdentifier
	emailAddress
Legal	companyId
	companyLegalName
	companyLegalIdentifier

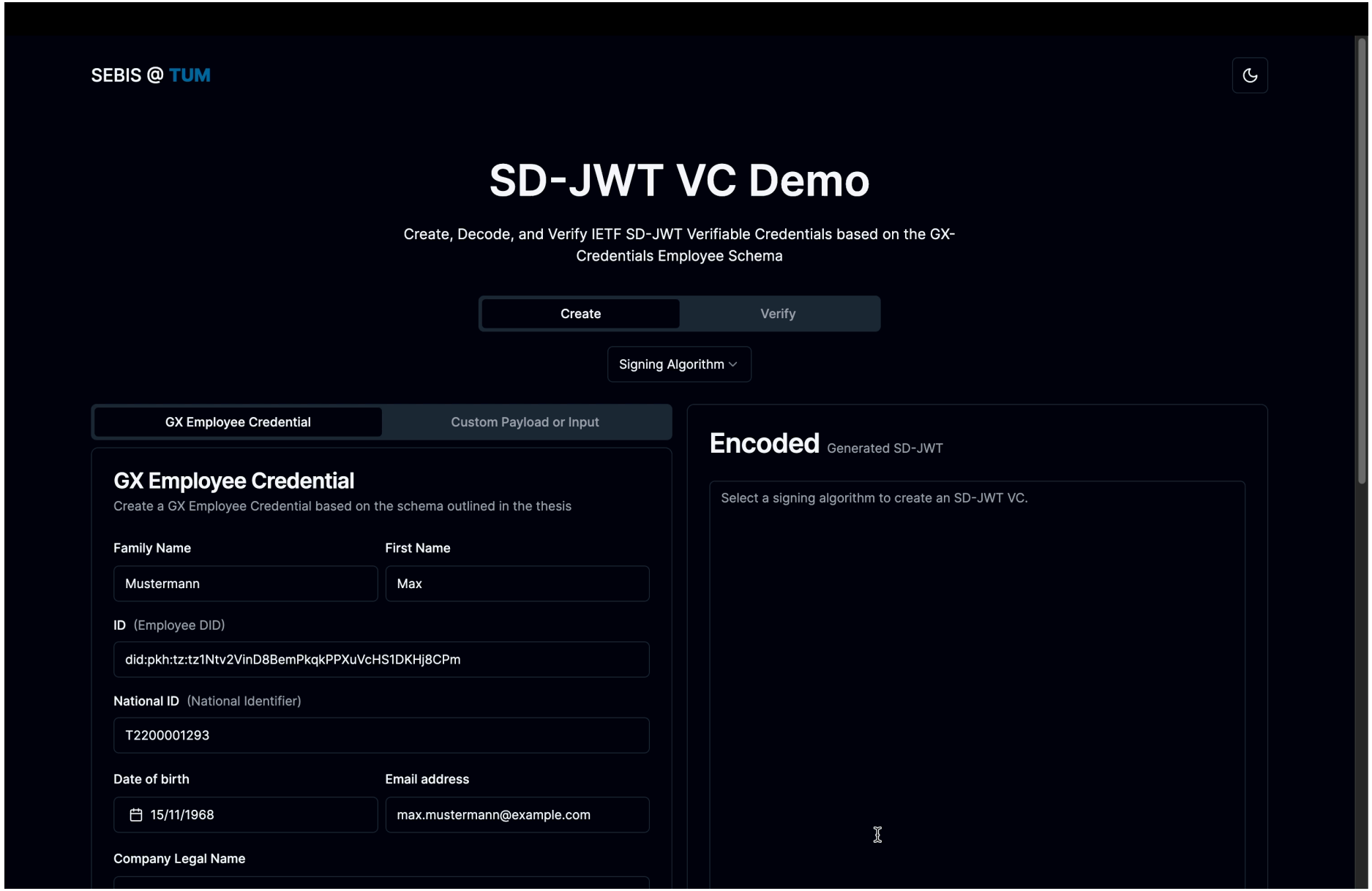
✅ ID binding (with Gov-ID)

✅ VC schema for natural subjects

RQ3: Engineering Effective Identity Credentials – Discussion



RQ3: Engineering Effective Identity Credentials – SD-JWT VC Demo



Video and live commentary

Limitations and Future Work

Literature Review & Taxonomy	• Researcher bias • Search results
Proposed Changes	• Ongoing development of standards and specifications
GX Credentials	• Issue SD-JWT VCs • Adopt OID4VC protocols

Summary

RQs

RQ1: What are the existing solutions and proposals for including identifying information in VCs?

RQ2: How can updates to identifying information be handled in VCs?

RQ3: How can we engineer effective identity credentials within the GX-Credentials project?

Key Results

- Taxonomy of 35 SSI approaches
- Findings
  - Gov-ID dominant
  - Revocation & SD

- Summarized (potential) update mechanisms
- Re-issuance is adequate

- Employee Identity Credentials
- SD-JWT VC
- OID4VCI Workflow
- Demo playground

Evan Christopher
evan.christopher@tum.de

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

wwwmatthes.in.tum.de

Literature Review: Search Strings

IEEE

(("Document Title": "Self-sovereign identity" OR "SSI") OR ("Document Title":identity management)) AND (("Full Text .AND. Metadata":natural person) OR ("Full Text .AND. Metadata":legal person) OR (“Full Text .AND. Metadata”:”person”)) AND ("Full Text .AND. Metadata":"verifiable credentials")

ACM

(Title:("self-sovereign identity" OR "SSI" OR identity management) AND (AllField:("natural person" OR "legal person") OR AllField: ("person")) AND Full- text:("verifiable credentials")

Search

“verifiable credentials "natural person" self sovereign identity "Identity Management" "natural person" "legal person" person

Scopus

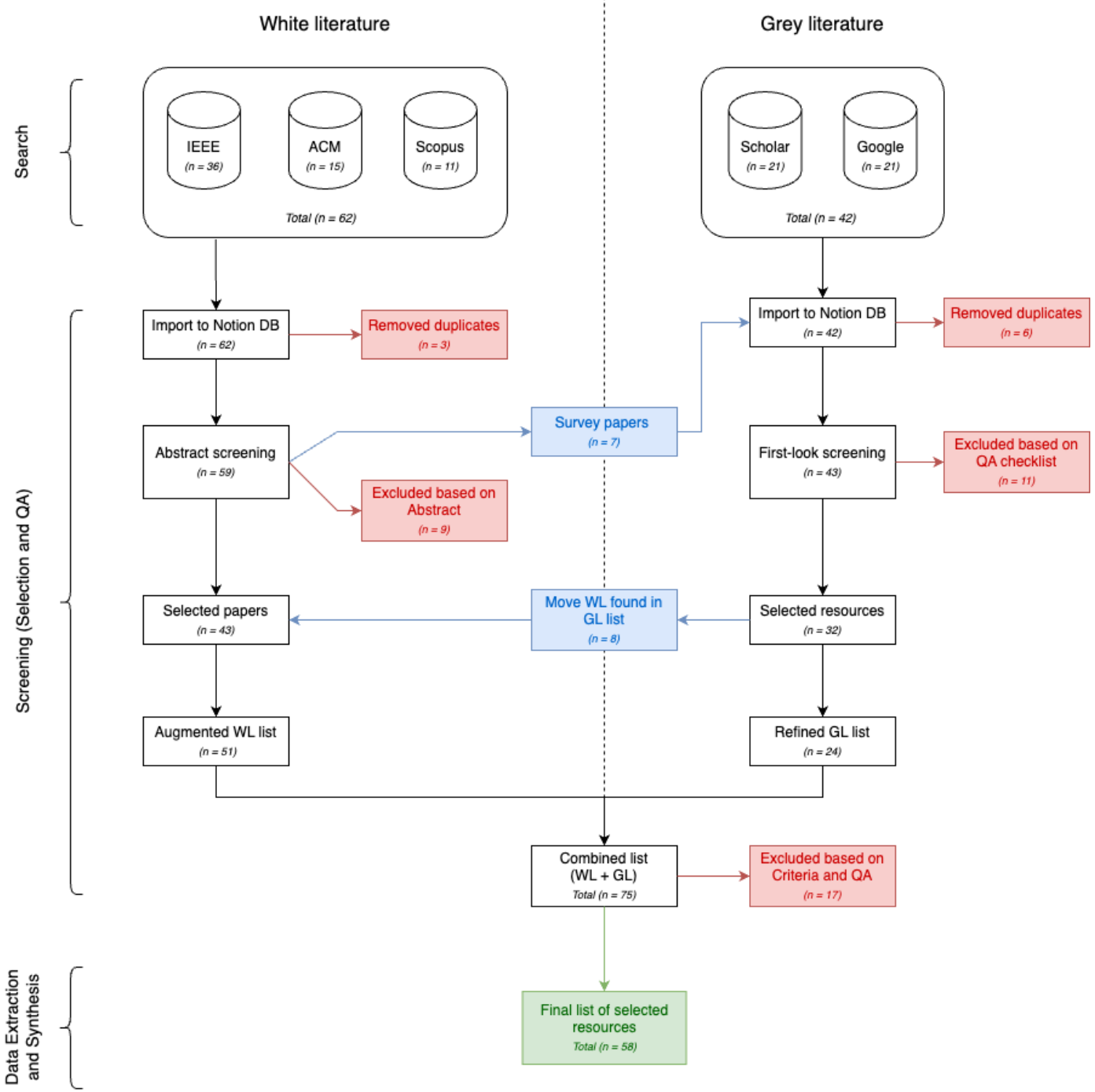
(TITLE ("self-sovereign identity" OR "SSI" OR "identity management") AND ALL ("natural person" OR "legal person" OR "person") AND ALL ("verifiable credentials"))

Scholar

“verifiable credentials" “self-sovereign identity” "Identity Management" "natural person" "legal person”

Literature Review Overview

Literature Review Process



Literature Review Overview

Literature Review: Quality Assessment Table for GL

Table 4.3.: Quality assessment table for GL.

Criteria	Questions
Authority of the producer	Is the publishing organization or author reputable and has expertise in the area?
Methodology	Is the source supported by authoritative, documented references?
Date	Does the resource have a clearly stated date and is published during the target period?
Relevance	Does the resource describe anything related to making a connection from natural subjects to VC-based digital identities?

Literature Review Overview

Taxonomy Construction: Objective Ending Conditions

Objective Ending Condition	Comment
All SSI approaches found from the survey deemed to be relevant have been examined	The survey includes both WL and GL. Both of these sources together provide an initial total of 92 SSI approaches before further refinement. Nevertheless, it is still considered an extensive sample that encapsulates existing SSI approaches since the inception of the concept.
No object was merged with a similar object or split into multiple objects in the last iteration	If objects were merged or split, then we need to examine the impact of these changes and determine if changes need to be made in the dimensions, characteristics, or the assigned objects.
At least one object is classified under every characteristic of every dimension	Should an object be unassignable to a characteristic due to incomplete information, it will be assigned to an 'unspecified' characteristic instead of making assumptions about the object and sacrificing objectivity.
No new dimensions or characteristics were added in the last iteration	If new dimensions were found, then more characteristics of the dimensions may be identified and vice versa. Adding new dimensions might also entail the deletion of other dimensions deemed superfluous.
No dimensions or characteristics were merged or split in the last iteration	The merging or splitting of dimensions or characteristics will have effects on the rest of the taxonomy. Its impact should be considered and changes made accordingly.
Every dimension is unique and not repeated	Duplicate dimensions need to be removed as they do not increase the value of the taxonomy.
Every characteristic is unique within its dimension	The removal of duplicate characteristics is necessary as we might have several dimensions with an "unspecified" characteristic.
Each combination of characteristics is unique and is not repeated	If cells are not unique, then there is redundancy/duplication in cells that need to be eliminated

Taxonomy Construction Overview

Taxonomy Construction: Subjective Ending Conditions

Subjective Ending Condition	Comment
Concise	The taxonomy should be informative without being overwhelming. We followed the suggested rule of thumb of seven plus minus two dimensions, but this isn't an objective ending condition, meaning the number can be exceeded if the addition of dimensions is deemed necessary.
Robust	The combination of dimensions and characteristics should be chosen to provide informative differentiation among objects of interest.
Comprehensive	The taxonomy is considered to be comprehensive once all dimensions of all objects of interest are identified, namely all relevant attributes of an identification approach for SSI solutions.
Extendible	Taxonomy extensibility is kept in mind during its construction to keep up with the rapid development in the SSI space. Should new information or details surface, the "unspecified" characteristic can be removed and replaced with new identified characteristics. New dimensions could also be added to extend the taxonomy.
Explanatory	We want to create a taxonomy that provides sufficient details on user identification approaches within the SSI context, including technical and non-technical information.

Taxonomy Construction Overview

Taxonomy

Table 5.3.: Proposed Taxonomy of SSI Approaches

Non-exclusive/ Exclusive	E	N	N							N				N				N			N		E		E		
SSI approaches	PII Location		PII Type		Identification Data Source						Identification Authority				Projected Cost per User				VC Format			Schema Standard		Selective Disclosure		Credential Revocation		
	Standalone	Bundled	Natural	Alternative	Gov-ID	Non-Gov-ID	Biometrics	PoP	None	Unspecified	End-user-asserted	Third-party asserted	SSI-Integrator asserted	First-party asserted	Free	Per-issuance + operation	Recurring base fee	Unspecified	LDP-VC	JWT-VC	Unspecified	Standardised	Flexible	Yes	No	Yes	No	Unspecified
Civic	x		x	x	x	x	x	x				x	x			x	x		x	x			x	x		x		
Jolocom		x	x	x						x	x				x						x		x	x		x		
Midy (Evernym)	x		x		x		x					x			x						x		x		x			x
Soltani et al. [112]	x		x	x	x									x		x					x		x		x	x		
MediLinker	x		x	x	x	x								x				x			x		x		x	x		
Alastria ID	x		x		x	x							x			x	x		x			x		x		x		
Tahlil et al. [49]		x	x		x									x				x			x		x	x		x		
Blockcerts		x	x						x		x					x			x				x		x	x		
Cosmos Cash		x	x						x		x							x	x				x		x			x
Dock		x	x	x	x	x	x						x			x	x		x	x			x	x		x		
Saidi et al. [113]		x		x					x		x							x			x		x		x	x		
Herbkle et al. [114]		x	x	x		x								x				x	x			x			x			x
Hamer et al. [115]	x		x				x					x						x	x				x		x	x		
Stockburger et al. [116]	x		x	x	x									x	x						x		x	x			x	
Wang et al. [117]		x		x	x							x						x			x		x		x			x
WeIdentity		x		x	x									x				x	x				x	x		x		
Xu et al. [118]	x			x					x		x							x			x		x		x	x		
M. Morosi [119]		x	x		x									x				x	x				x	x		x		
C. Sehlke [26]	x		x		x	x								x	x				x			x			x	x		
Trinsic		x	x	x	x	x	x						x			x			x	x			x	x		x		
ValID		x	x	x					x		x				x						x		x		x	x		
Altme		x	x		x	x		x				x			x				x	x		x	x		x			x
Datakeeper	x		x		x	x	x						x			x	x		x				x	x		x		
Gataca.io		x	x	x	x	x	x	x					x			x	x		x	x		x	x	x		x		
GlobalID		x	x	x	x	x	x	x				x	x			x					x		x		x	x		
Indicio Proven		x	x	x	x	x	x	x					x			x					x		x	x		x		
Lissi		x	x	x	x	x							x			x	x				x		x	x		x		
Mattr		x	x	x	x	x	x						x				x		x			x	x	x		x		
Meeco		x	x	x					x				x				x			x			x	x			x	
Verida	x		x		x	x							x			x				x			x	x				x
VIDchain	x		x						x				x					x		x		x	x	x		x		
Walt.id	x		x	x					x				x					x	x			x	x		x	x		
Belchior et al. [120]		x	x						x					x	x						x		x	x		x		
Rahman et al. [121]	x		x		x									x				x			x		x	x				x
Satybaldy et al. [122]		x	x	x	x	x								x				x	x			x		x		x		

Taxonomy Overview

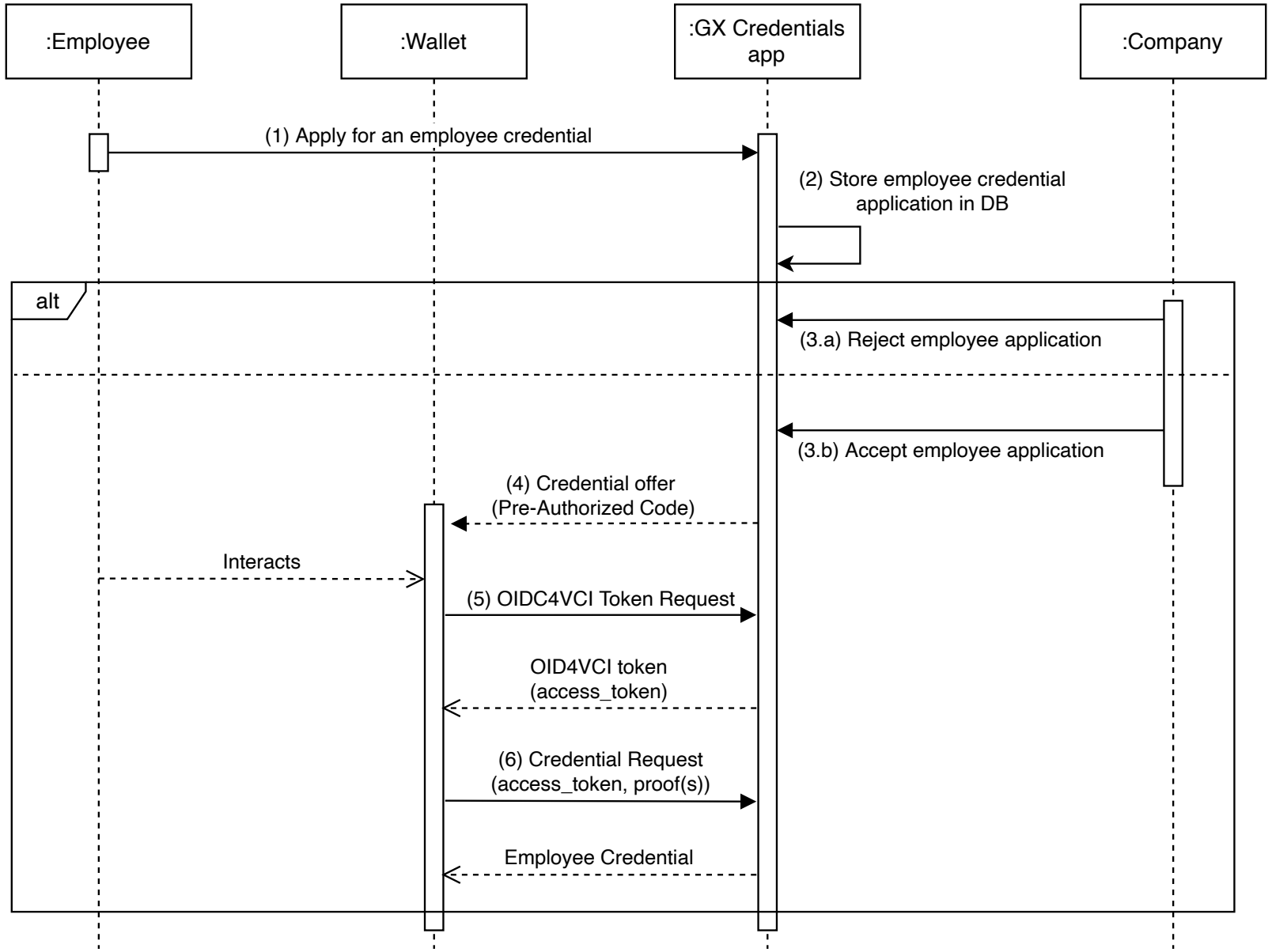
Proposed GX Employee Credential

Property	Description	eIDAS Minimum Data Set Property and Description
`id`	Defines the DID of the employee	✗
`familyName`	Defines the current family name(s) of the employee	✓, *current family name*
`firstName`	Defines the current first name(s) of the employee	✓, *current first name*
`dateOfBirth`	Defines the date of birth of the employee	✓, *date of birth*
`nationalIdentifier`	Defines the unique national identifier of the employee	✓, *uniqueness identifier*
`emailAddress`	Defines the employee's email address according to the company's domain name used for correspondence	✗
`companyId`	Defines the ID (DID) of the issuing company	✗
`companyLegalName`	Defines the legal name of the company that issued the employee credential	✓, *current legal name*
`companyLegalIdentifier`	Legal identifier as proposed by [165], in our case derived from the employee's VAT identification number	✓, as the ID may be derived from VAT registration number, tax reference number, LEI, EORI, SIC (the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council), SEED (excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012) [102].

Table 7.2.: Identity Attributes Included in the Proposed GX Employee Credential

Employee Credential Overview

Employee Credential Issuance in GX-Credentials with OID4VCI Pre-Authorized Code Flow



Workflow Proposal

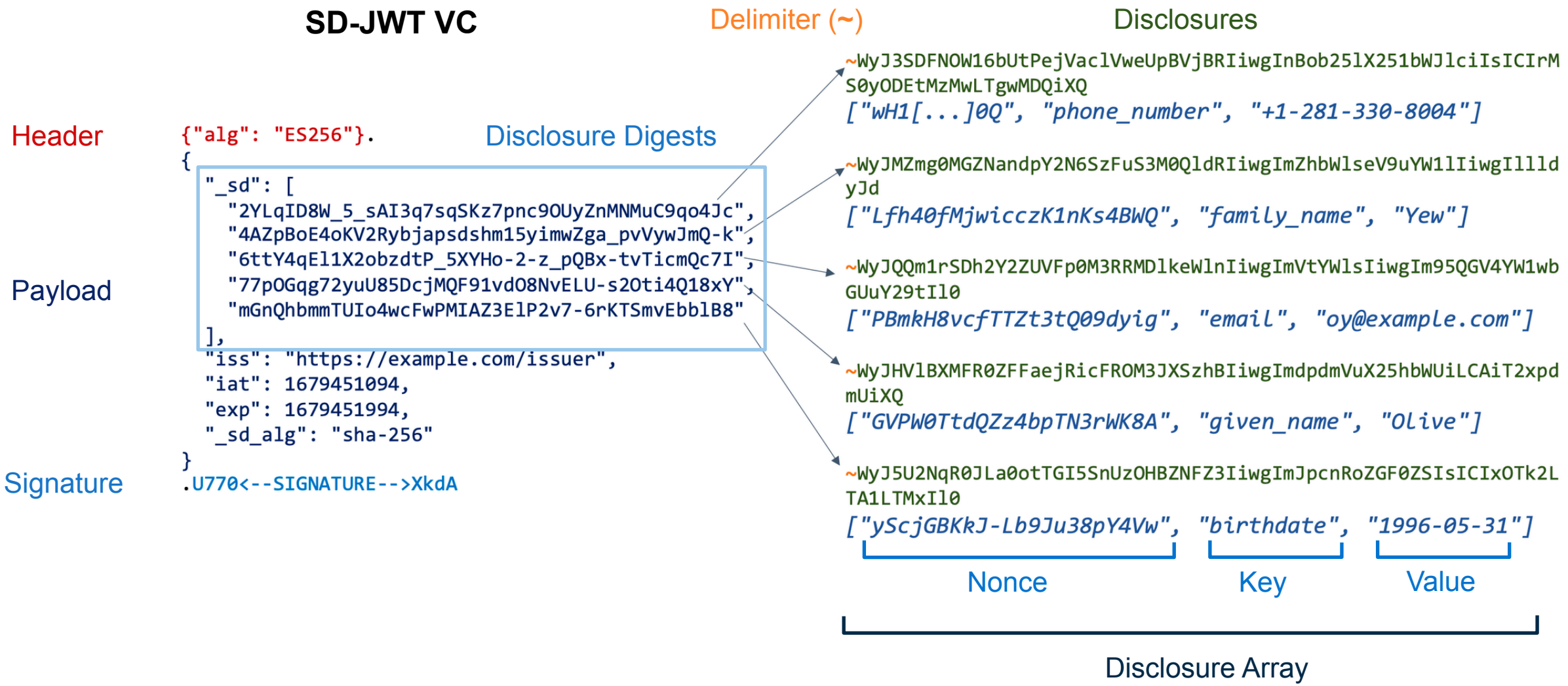
Library Evaluation

Library or Reference Implementation	SD Draft version	Ease of Use	Documentation	Test cases	Programming Language	GitHub Stars
christianpaquin/sd-jwt [171]	3	Medium	Good	✓	TypeScript	12
berendsliechtrecht/sd-jwt-ts [172]	5*	Medium	None	✓	TypeScript	6
chike0905/sd-jwt-ts [173]	2	Medium	Good	✓	TypeScript	5
Meeco/sd-jwt-vc [174]	5	Easy	Very Good	✓	TypeScript	0
transmute-industries/vc-jwt-sd [175]	5*	Medium	Good	✓	TypeScript	3
openwallet-foundation-labs/sd-jwt-python [176]	5	Medium	Very Good	✓	Python	4
authlete/sd-jwt [177]	4	Easy	Very Good	✓	Java	13
walt-id/waltid-sd-jwt [178]	4	Medium	Good	✓	Kotlin (Multiplatform)	7

Table 7.3.: Evaluation of SD-JWT Libraries

Demo Overview

SD-JWT VCs



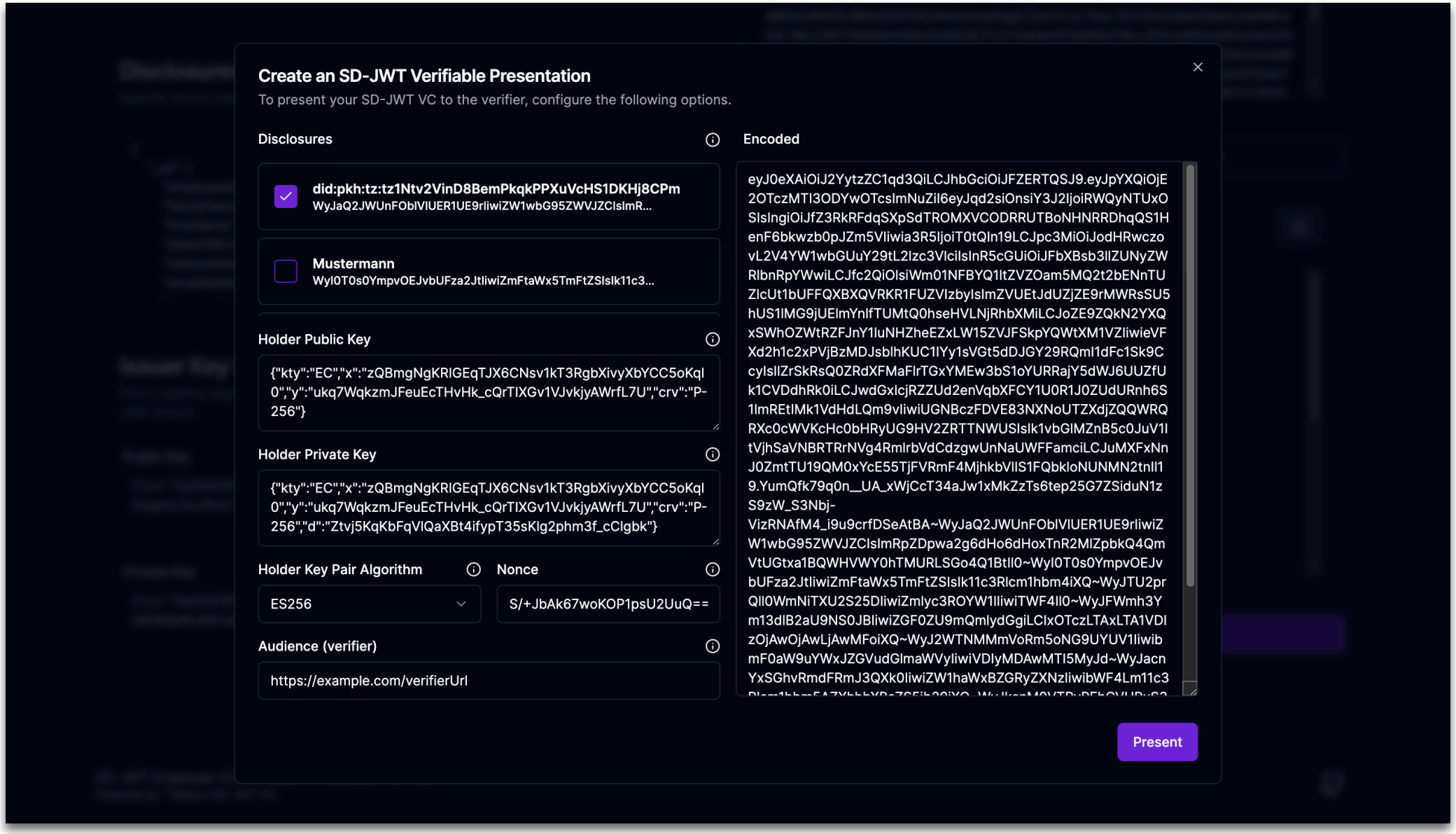
SD-JWT VC Overview

Image source: https://datatracker.ietf.org/meeting/117/materials/slides-117-oauth-sessb-sd-jwt-00

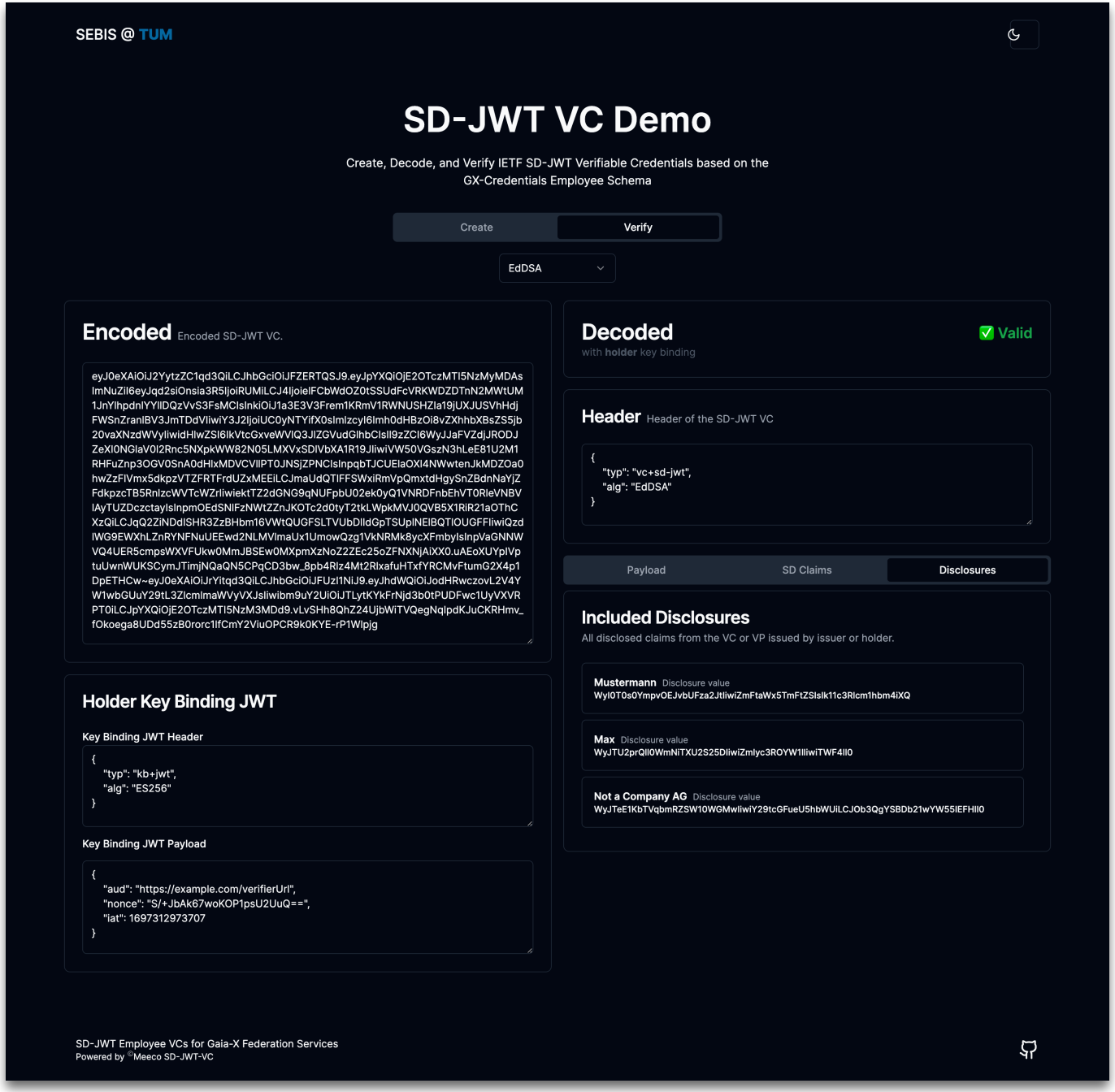
SD-JWT VC
Demo UI (1/5)

SD-JWT VC
Demo UI (2/5)

SD-JWT VC Demo UI (3/5)



SD-JWT VC Demo UI (4/5)



SD-JWT VC Demo UI (5/5)