The State of the Art and Practice of Digital Credentialing

Dominik Gerbershagen, March 30th 2020, Master’s Thesis Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Agenda

1. Motivation

2. Research Questions and Approach

3. Findings
    - 3a. State of the Art
    - 3b. State of the Practice
    - 3c. Analysis

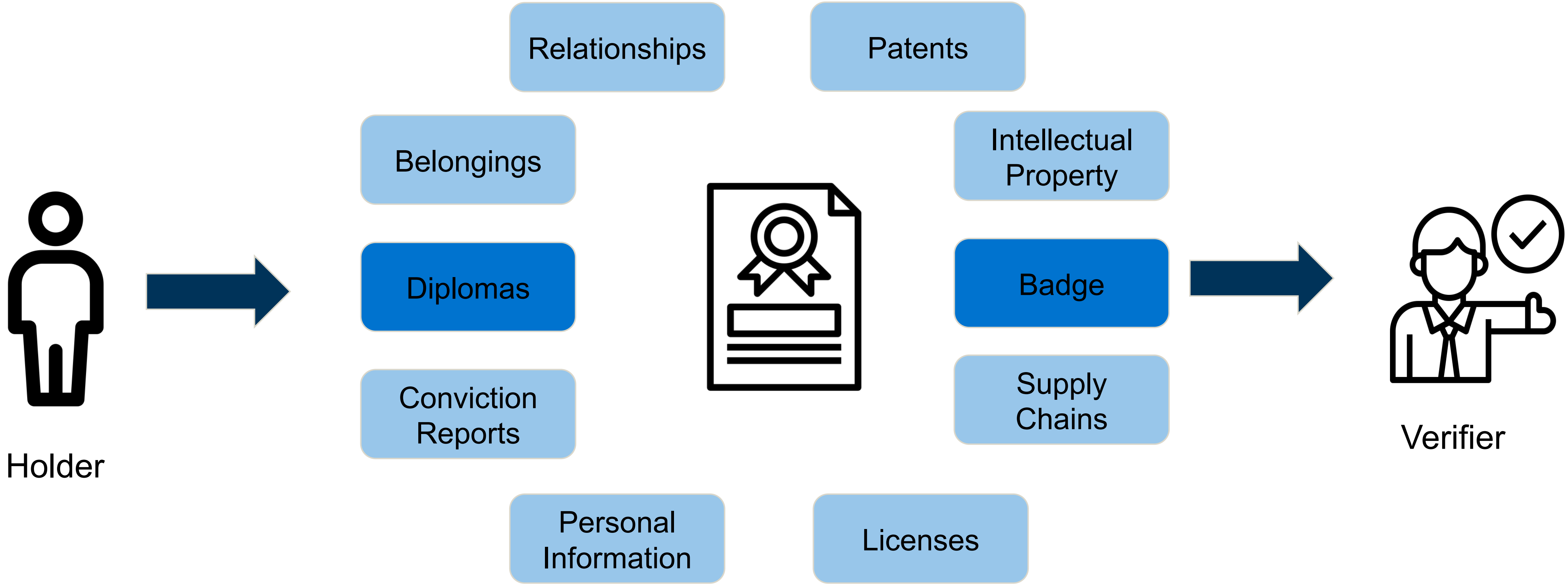
4. Limitations

5. Conclusion

6. Future Work

Problem Statement

How can someone trust that the credential is valid and unforged?



Research Questions

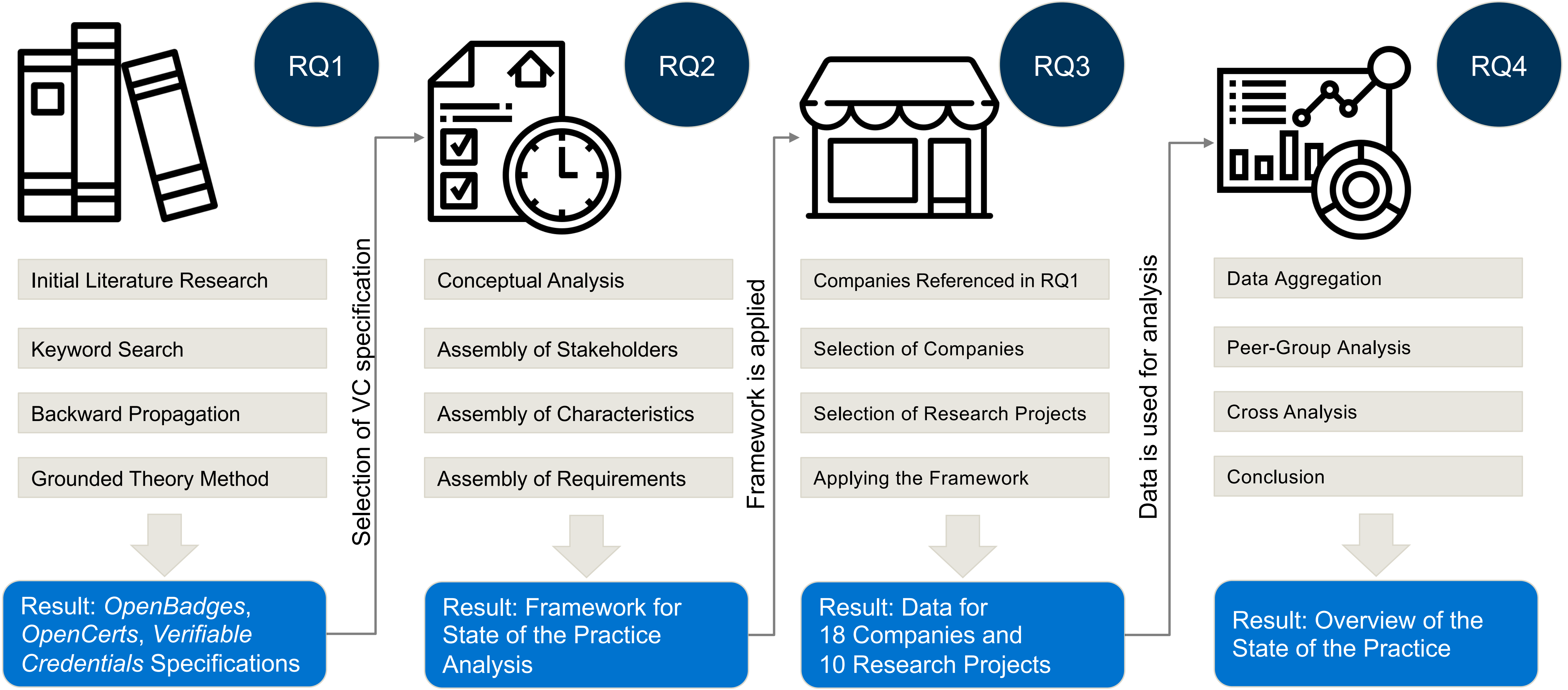
RQ1 What is the current state in terms of standardization for digital credentialing?

RQ2 What requirements and processes have to be in place to create a digital credentialing system?

RQ3 Which companies and research projects are already participating in the market for digital credentialing?

RQ4 What are the differences and similarities of these companies and projects?

Research Approach



RQ1

- Initial Literature Research
- Keyword Search
- Backward Propagation
- Grounded Theory Method

Result: *OpenBadges*, *OpenCerts*, *Verifiable Credentials* Specifications

Selection of VC specification

RQ2

- Conceptual Analysis
- Assembly of Stakeholders
- Assembly of Characteristics
- Assembly of Requirements

Result: Framework for State of the Practice Analysis

Framework is applied

RQ3

- Companies Referenced in RQ1
- Selection of Companies
- Selection of Research Projects
- Applying the Framework

Result: Data for 18 Companies and 10 Research Projects

Data is used for analysis

RQ4

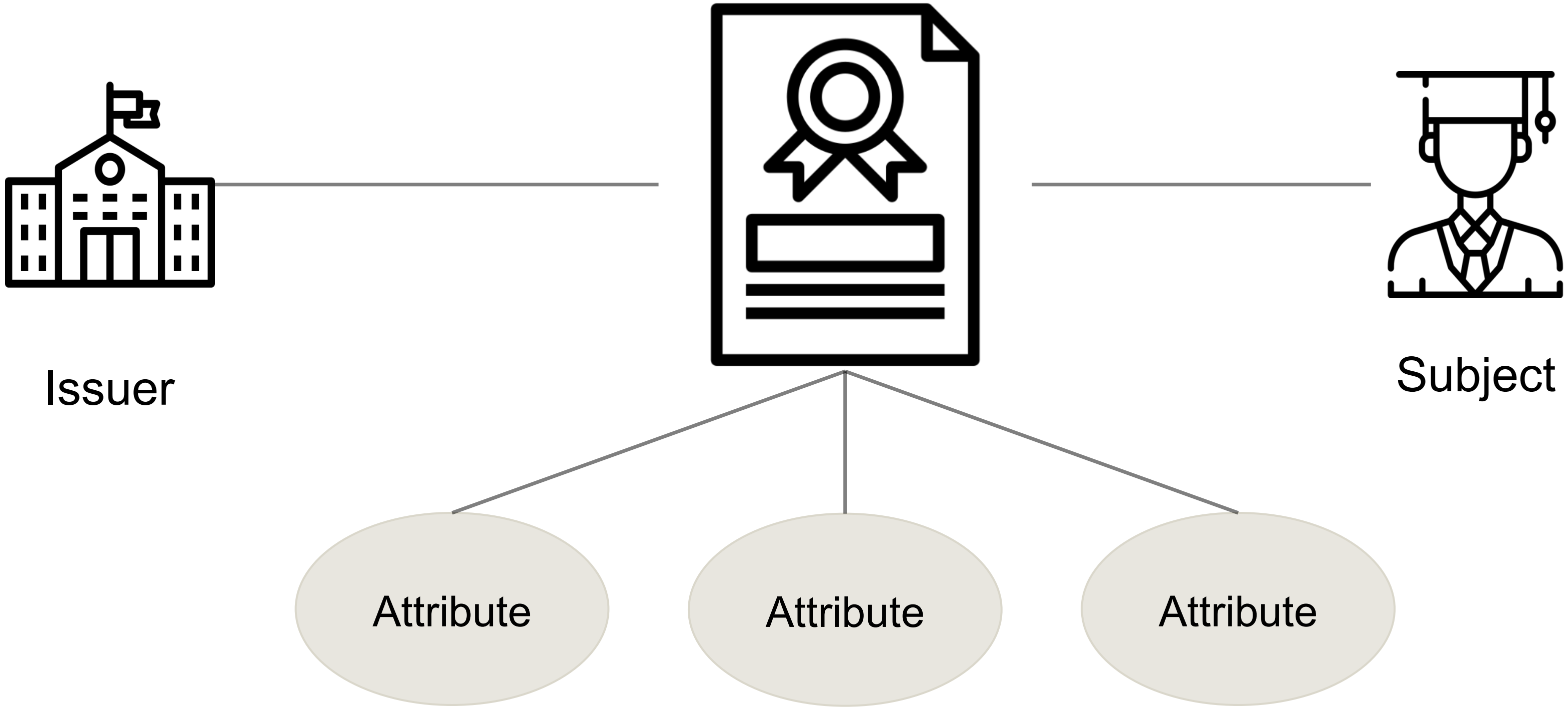
- Data Aggregation
- Peer-Group Analysis
- Cross Analysis
- Conclusion

Result: Overview of the State of the Practice

Definition of Credential

RQ1

„an assertion by an issuer of some attributes of the subject of the credential“ [10]



Findings – State of the Art

RQ1

Standardizing Specifications

W3C Verifiable Credentials Draft [1]	IMS OpenBadges [2]	OpenCerts [3]
Focus on Macro-Credentials	Focus on Micro-Credentials	Implementation Framework
Concepts for multiple Industries	Rather Tied to Education	Macro- & Micro-Credentials
Embedded Proofs	Widely adopted	No Standardization Focus
Technology Independent	Depends on HTTP for Proofs	No Interoperability

State of the Art – Conceptual Comparison

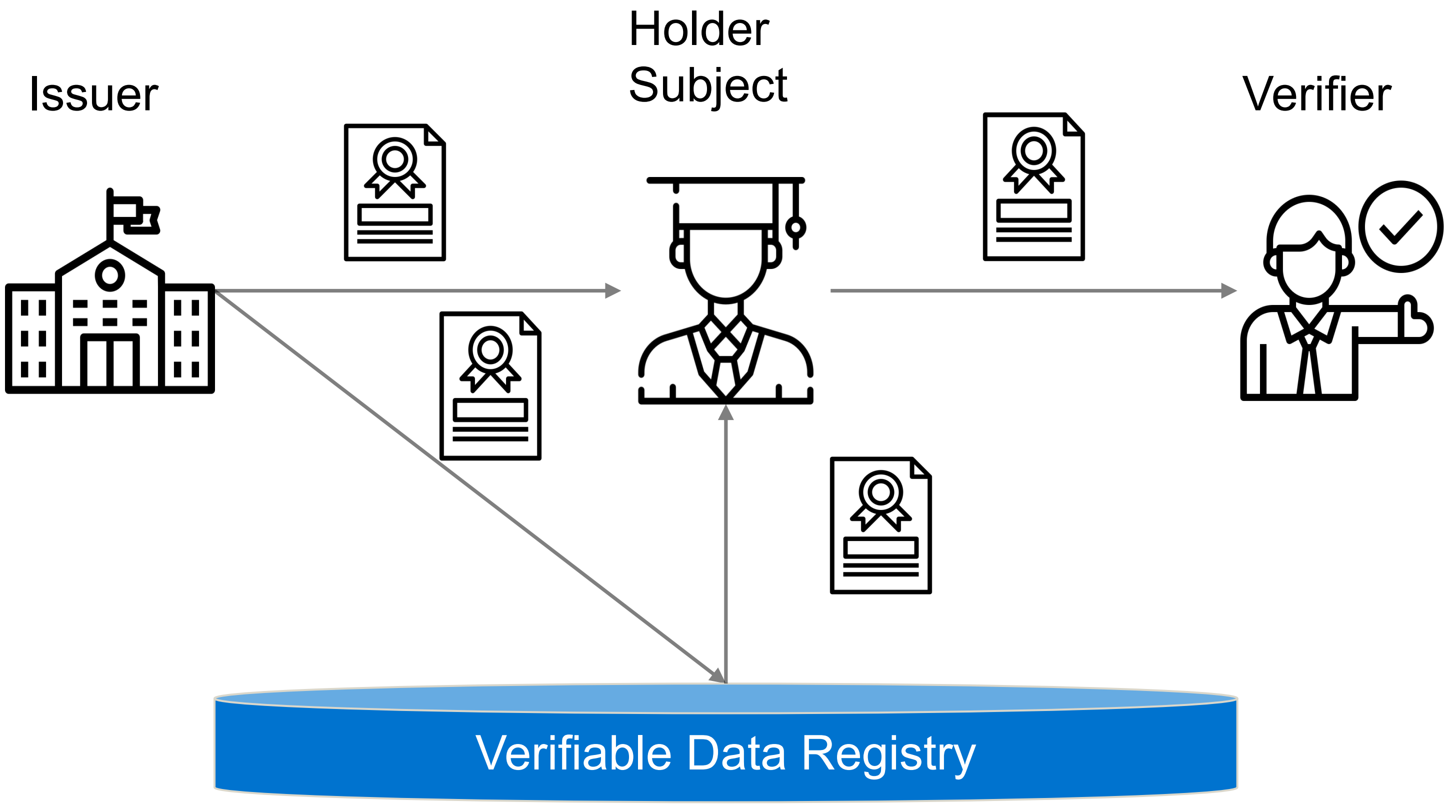
RQ2

	Concept	Verifiable Credentials	OpenBadges	OpenCerts
Basic Concepts	Identifiers	Yes	Yes	Yes
	Types	Yes	Yes (only one type)	No
	Subject	Yes	Yes	Yes
	Issuer	Yes	Yes	Yes
	Issuance Date	Yes	Yes	Yes
	Proofs	Yes	No	No
	Expiration	Yes	Yes	No
	Status	Yes	Yes (implicit)	No
Advanced Concepts	Extensibility	Yes	Yes	No
	Refreshing	Yes	No	No
	Terms of Use	Yes	No	No
	Evidence	Yes	Yes	No
	Zero-Knowledge Proofs	Yes	No	No
	Disputes	Yes	No	No

Order taken from [1], data from [1], [2], [3].

State of the Art – Stakeholders

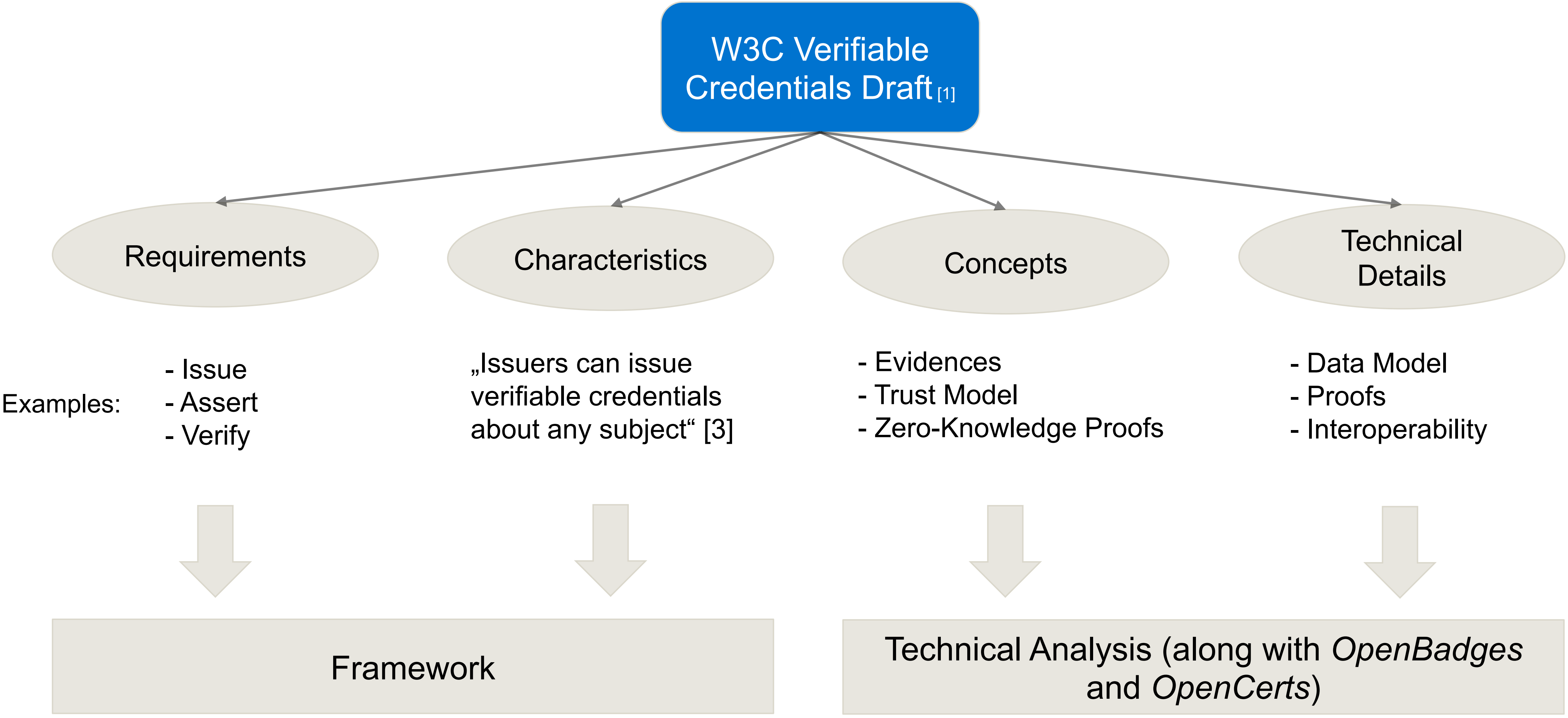
RQ2



[1]

RQ2

State of the Art – Extraction Methodology



W3C Verifiable Credentials Draft [1]

Requirements

Characteristics

Concepts

Technical Details

Examples:
- Issue
- Assert
- Verify

„Issuers can issue verifiable credentials about any subject“ [3]

- Evidences
- Trust Model
- Zero-Knowledge Proofs

- Data Model
- Proofs
- Interoperability

Framework

Technical Analysis (along with *OpenBadges* and *OpenCerts*)

[3], [4]

State of the Art – Framework

RQ2

Requirements

- Issue
- Assert
- Verify
- Store
- Move
- Retrieve
- Revoke

Actions

- Issue
- Store
- Move Claim
- Refresh
- Revoke
- Receive
- Assemble
- Interact
- Verify
- Surroundings

System

- Data Model
- Permission
- Data Storage Model
- References
- Macro- / Micro-Credential Compatibility
- GDPR Compliance
- API Available
- Meta Data Support
- Identification Method
- Trust Model

Business

- Business Model
- Usage KPIs
- Cooperations / Partners
- Maturity
- Target Industry

[4]

State of the Art – Technical Analysis

RQ2

```
{
        "@context": [
                "https://www.w3.org/2018/credentials/v1",
                "https://www.w3.org/2018/credentials/examples/v1"
        ],
        "id": "http://tum.de/credentials/3732",
        "type": ["VerifiableCredential", "UniversityEnrollment"],
        "issuer": "https://tum.de",
        "issuanceDate": "2020-04-01T10:09:59Z",
        "expirationDate": "2020-09-30T23:59:59Z",
        "refreshService": {
                "id": "https://tum.de/refresh/3732",
                "type": "StudentIdRefreshService"
        },
        "credentialSubject": {
                "id": "did:tum:ebfeb1f712ebc6f1c276e12ec21",
                "studentEnrollment": {
                        "id": "did:gerbershagen:abcd1f712ebc6f1c276e12ec21",
                        "name": "Dominik Gerbershagen",
                        "studyProgram": "Master of Science Information Systems",
                        "semester": 6
                }
        },
        "proof": {
                "type": "RsaSignature2018",
                "created": "2019-06-10T10:09:59Z",
                "proofPurpose": "assertionMethod",
                "verificationMethod": "https://tum.de/credAssertion/keys/1",
                "jws": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOls"
        }
}
```

Extensibility and Interoperability

Basic credential data

Automatic refreshment of Credential

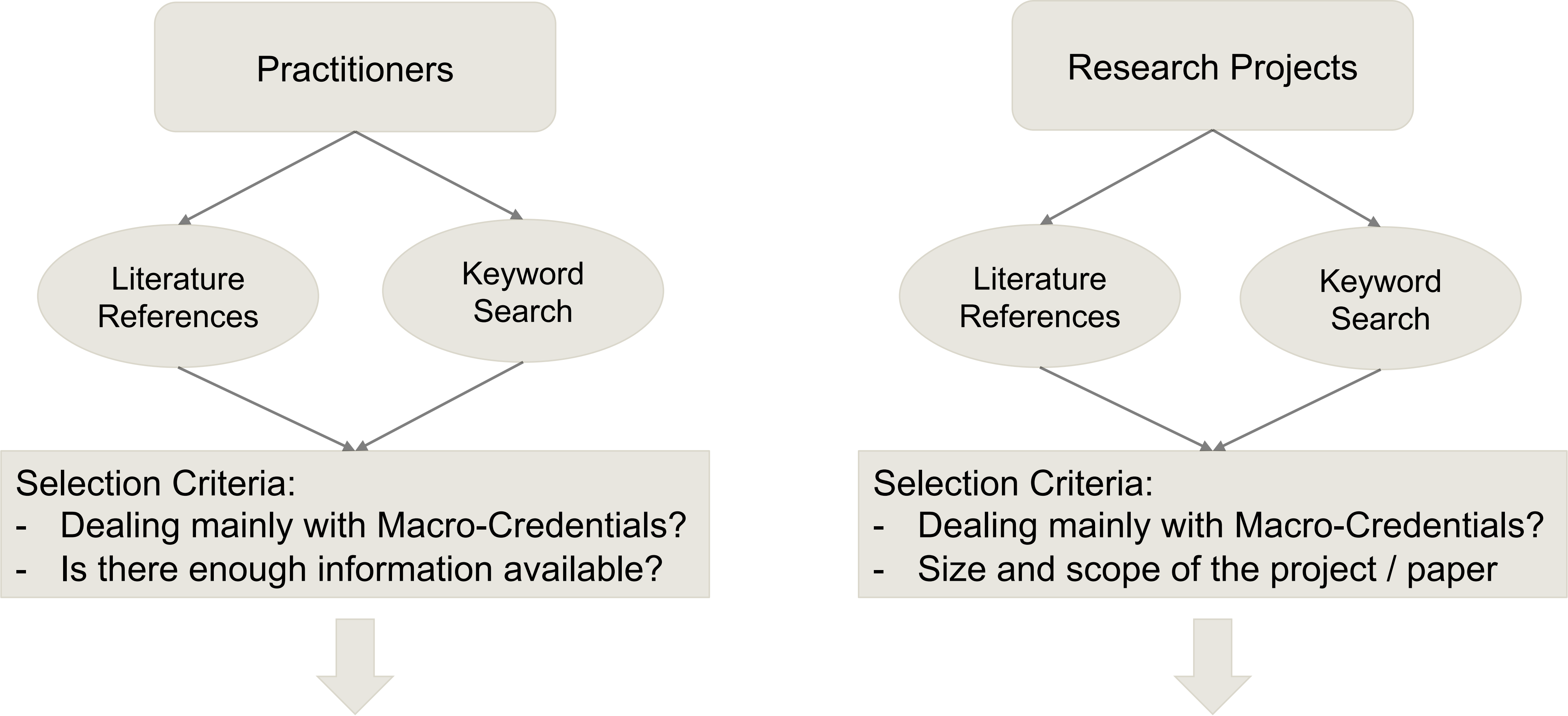
Information about the subject that is credentialed

Embedded Proof to automatically verify authenticity and integrity of the credential

W3C Verifiable Credentials Draft – Example Credential with Refreshment Service [1].

State of the Practice – Practitioners and Research Projects

RQ3



Selection Criteria:
- Dealing mainly with Macro-Credentials?
- Is there enough information available?

Selection Criteria:
- Dealing mainly with Macro-Credentials?
- Size and scope of the project / paper

18 Practitioners

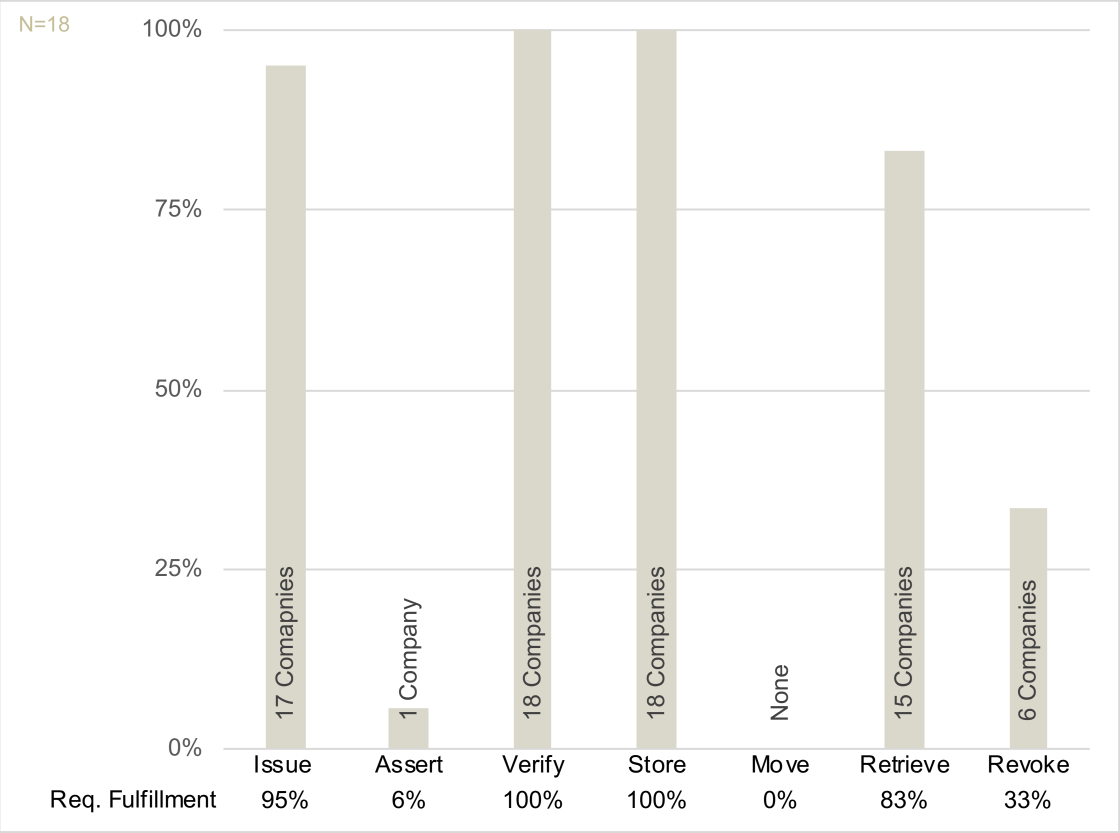
10 Research Projects

[4]

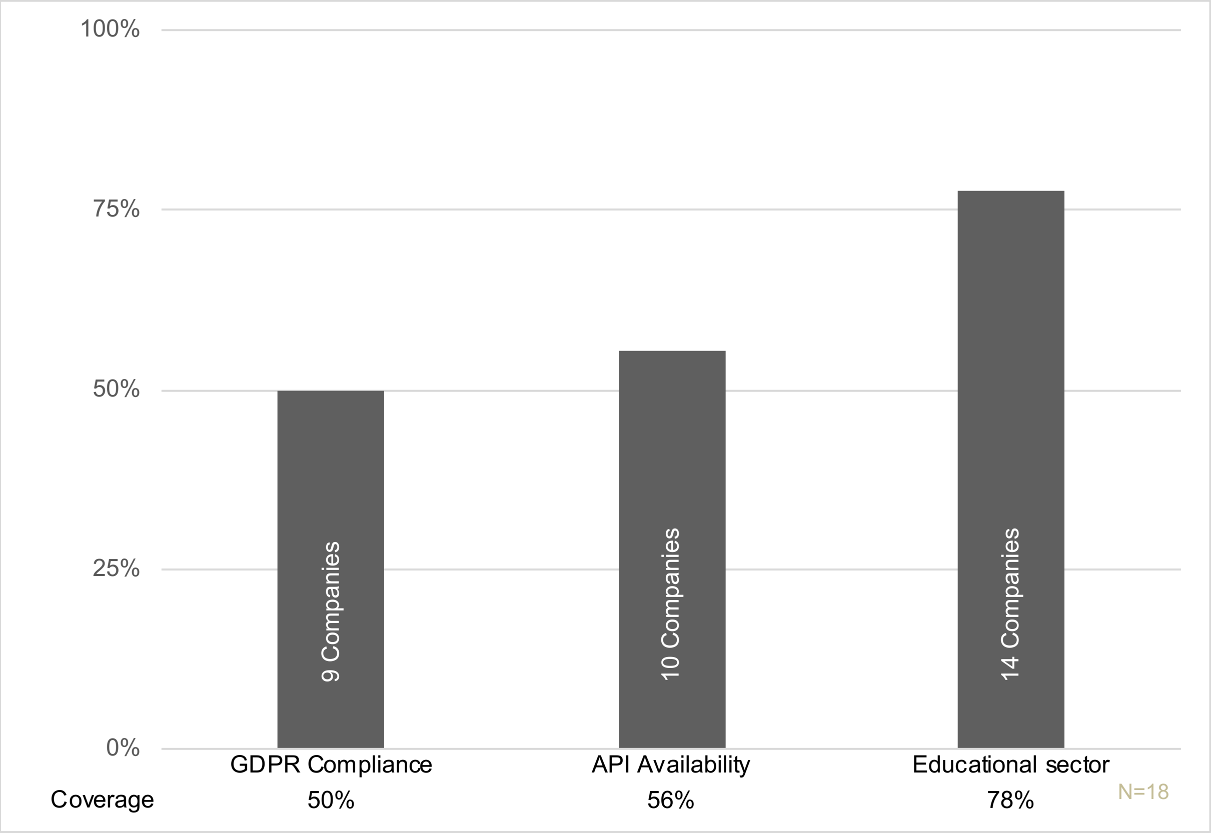
State of the Practice – Practitioner Analysis

RQ4

Requirement Fulfillment



GDPR Compliance, API Availability, Educational Sector

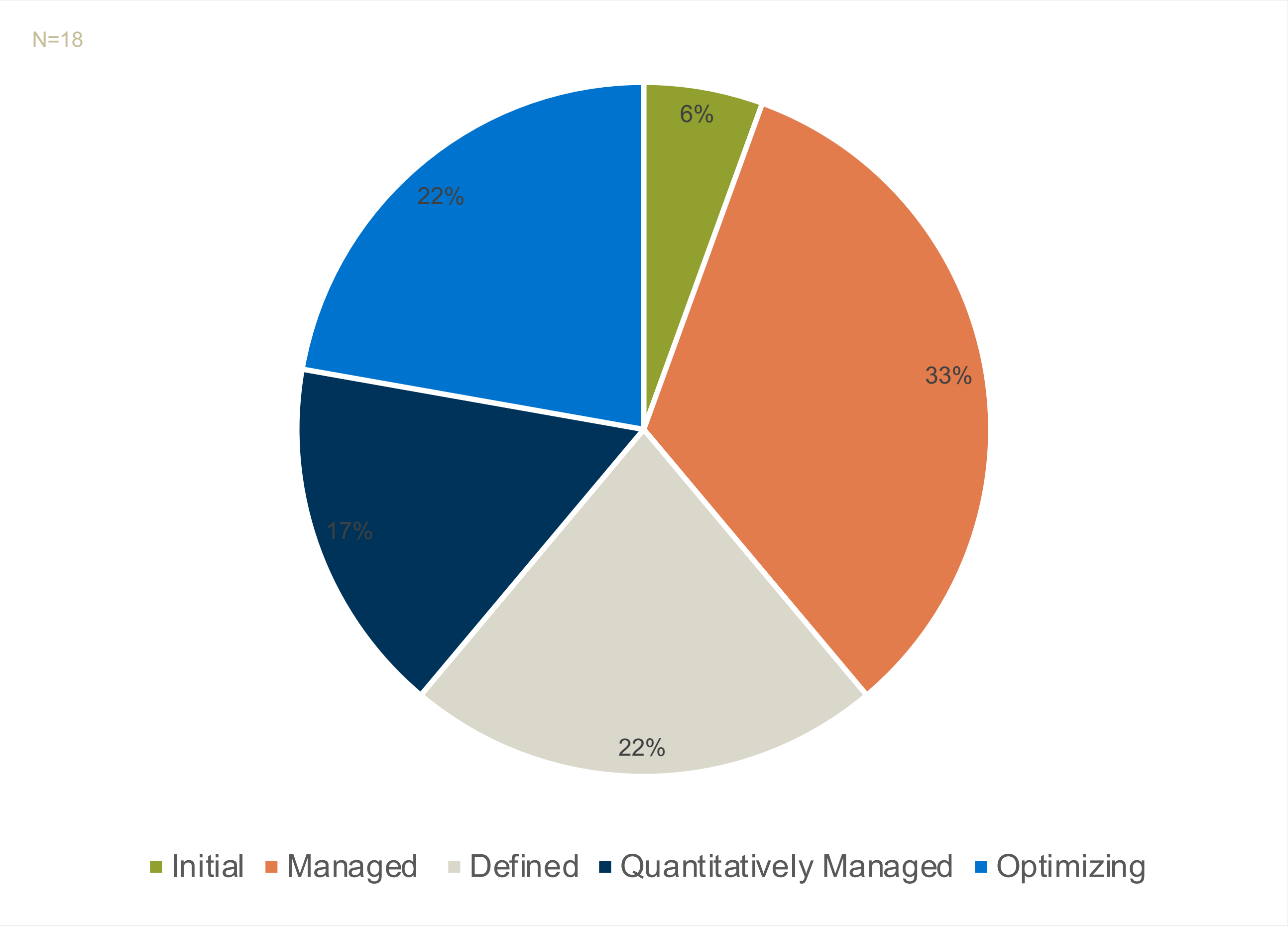


Motivation · Research Questions · Findings · Limitations · Conclusion · Future Work

State of the Practice – Practitioner Analysis

RQ4

Maturity of Companies based on CMMI [5], [6]



Motivation Research Questions Findings Limitations Conclusion Future Work

State of the Practice – Practitioner Analysis

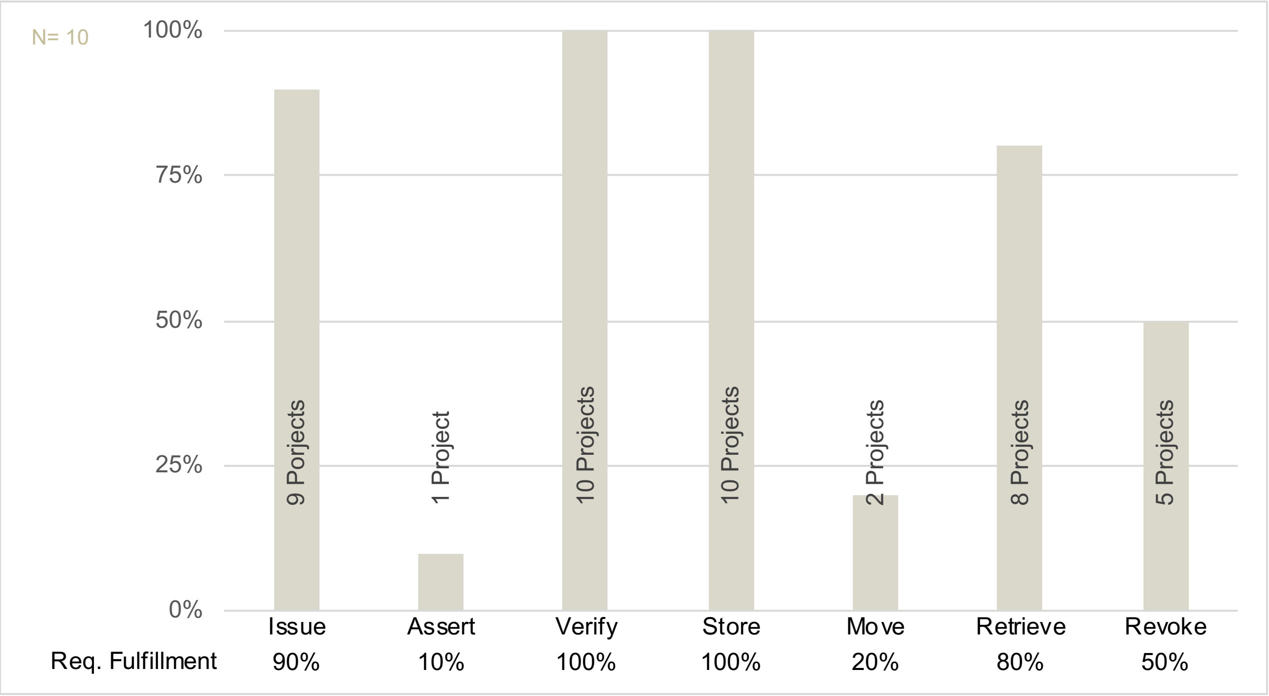
RQ4

- 17 out of 18 companies rely on blockchain technology
- 72% of the companies have permissionless approach (due to Blockchain implementation)
- 28% are OpenBadges compliant, only 1 out of 18 is compliant to Verifiable Credentials Draft (BlockCerts)
- 94% rely on a peer-to-peer trust model
- Advanced Concepts (Zero-Knowledge Proof, Moving Credentials, Disputes) could not be found among companies
- Credentials are stored in a central database, the hash is stored on-chain

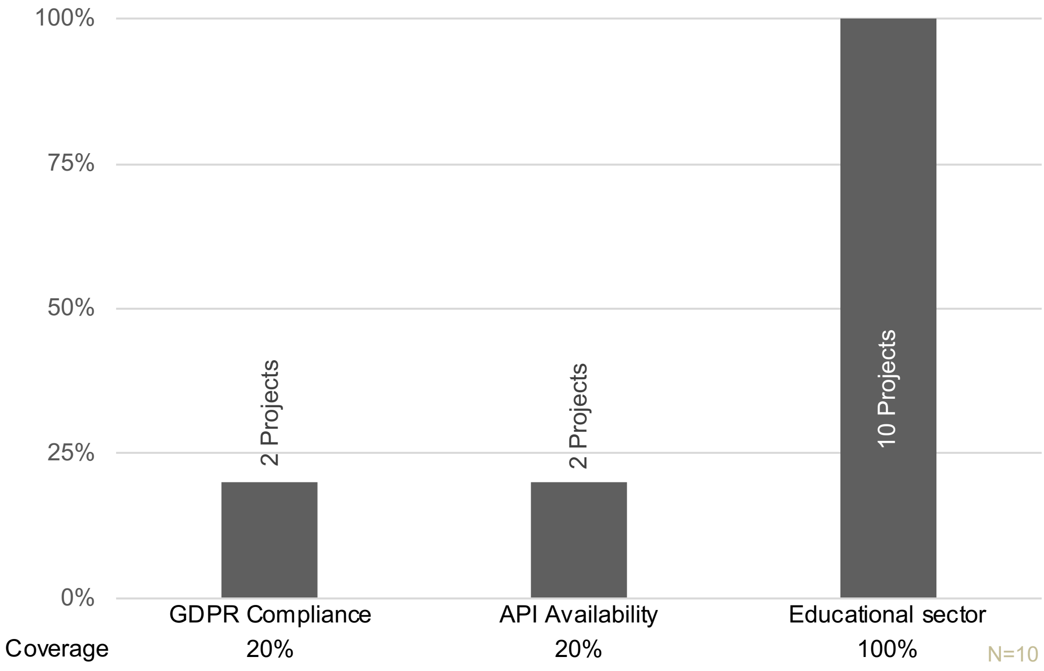
State of the Practice – Research Projects Analysis

RQ4

Requirement Fulfillment



GDPR Compliance, API Availability, Educational Sector



Motivation | Research Questions | Findings | Limitations | Conclusion | Future Work

State of the Practice – Research Project Analysis

RQ4

- 10 out of 10 Projects use Blockchain technology.
- 30% compliant to OpenBages, none compliant to Verifiable Credentials
- Tendency towards consortium (permissioned) blockchains (5 out of 10 projects)
- GDPR compliance and API availability are not as important as it is for businesses
- Advanced Concepts (Zero-Knowledge Proof, Moving Credentials, Disputes) could not be found among research projects
- Maturity of Research Projects is rated as “defined”

Limitations

- Maturity based on CMMI could only be assumed due to the lack of insight.
  - Reason: Lack of insight in the businesses.
  - Solution: Creation of a framework or interviewing practitioners to gather more data.

- The Framework worked well for practitioners, but not for research projects.
  - Reason: Research focuses mostly a certain aspect of a system instead of a complete solution.
  - Solution: Different framework solely for research projects.

- Lack of information that is publicly available for certain companies.
  - Reason: Early stage development, not yet publicly available product.
  - Solution: Interviewing these companies or re-investigation of the State of the Practice at a later point in time.

Conclusion

State of the Art

- OpenBadges widely adopted for micro-credentials, sometimes used for macro-credentials
- Verifiable Credentials Draft offer standardization for macro-credentials
- Domain of digital credentialing can divers into several industries apart from education
- Identification comes in separate layer, not included in standardization

State of the Practice

- Market is in early stage, businesses mostly small
- Common approach based on blockchain technology
- Research is rather focused on permissioned blockchains
- API availability and GDPR compliance critically for businesses, irrelevant for research
- Businesses have business model, data storage and actions in common
- W3C VC draft has not been adopted yet

Future Work

- Reviewing the State of the Practice:
  - How has the market changed?
  - How is the adoption rate for the Verifiable Credentials specification?

- Adaption of the Framework for research projects:
  - Suitable not only for whole systems, but also for certain aspects of it
  - Focus on system architecture

- Creating a prototype based on the Verifiable Credentials specification:
  - Implementation of advanced concepts
  - Creating a system that allows moving credentials to another one

Sources

Literature

[1] M. Sporny, D. Longley, and D. Chadwick. Verifiable Credentials Data Model 1.0. Tech. rep. W3C, 2019, pp. 1–115. URL: https://w3c.github.io/vc-data-model/ %20https://www.w3.org/TR/vc-data-model/.
[2] J. Bohrer, T. F. Cook, M. Esquela, S. Gance, J. Goodell, M. Gylling, V. Haag, A. Hripak, K. Lemoie, M. Leuba, R. Macdonald, N. Otto, J. Pitcher, S. Ravet, A. Reis, J. Schmidt, and A. Szabo-Nagy. Open Badges v2.0. 2018. URL: https://www.imsglobal.org/ sites/default/files/Badges/OBv2p0Final/index.html.
[3] Government Technology Agency. Documentations for opencerts. 2020. URL: https: //docs.opencerts.io/.
[4] S. Otto, S. Lee, B. Sletten, D. Burnett, M. Sporny, and K. Ebert. Verifiable Credentials Use Cases. Tech. rep. W3C, 2019. URL: https://www.w3.org/TR/vc-use-cases/.
[5] SEI. CMMI® for Development, Version 1.3 CMMI-DEV, V1.3 - Improving processes for developing better products and services. Tech. rep. 2010, p. 482. URL: http: //www.sei.cmu.edu.
[6] H. Wang, K. Chen, and D. Xu. "A maturity model for blockchain adoption". In: Financial Innovation 2.1 (2016). ISSN: 21994730. DOI: 10.1186/s40854-016-0031-z. URL: http://dx.doi.org/10.1186/s40854-016-0031-z.
[7] F. Office for Information Security. Overview of the German eID system. Tech. rep. 2017. URL: https://www.bsi.bund.de.
[8] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello. Decentralized Identifiers (DIDs) v1.0. 2019. URL: https://www.w3.org/TR/did-core/.
[9] M. Schäffner. "Analysis and Evaluation of Blockchain-based Self-Sovereign Identity Systems". Master thesis. Technical University of Munich, 2020.
[10] A. Herzberg and Y. Mass. "Relying party credentials framework". In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2020 (2001), pp. 328–343. ISSN: 16113349.

Sources

Icons

Page 3:
- Verifier: https://www.flaticon.com/authors/surang
- Holder: https://www.flaticon.com/authors/kiranshastry
- Credential: https://www.flaticon.com/authors/surang

Page 5 (left to right):
- https://www.flaticon.com/authors/mavadee
- https://www.flaticon.com/authors/surang
- https://www.flaticon.com/authors/freepik
- https://www.flaticon.com/authors/eucalyp

Page 7 (left to right):
- Issuer: https://www.flaticon.com/authors/good-ware
- Holder: https://www.flaticon.com/authors/freepik
- Verifier: https://www.flaticon.com/authors/surang
- Credential: https://www.flaticon.com/authors/surang

Page 32:
- Identifier: https://www.flaticon.com/authors/fjstudio
- Distributed Ledger: https://www.flaticon.com/authors/good-ware

B.Sc.

Dominik Gerbershagen
Student Master of Science Information Systems

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.   0
Fax +49.89.289.17136

Dominik.Gerbershagen@in.tum.de
wwwmatthes.in.tum.de

Backup

Used Keywords for Literature Review

RQ1

- Digital degree certificate
- Tamper-free digital degree certificate
- Digital signing services
- Digital credentialing
- Certification
- Certificate
- Blockchain
- Smart contract
- IPFS (InterPlanetary File System)
- BSCW (Basic Support for Cooperative Work)
- Blockcerts
- Certificate verification
- Educational Blockchain
- Educational record repository

State of the Art - Requirements

RQ2

W3C Verifiable Credentials Draft [1]

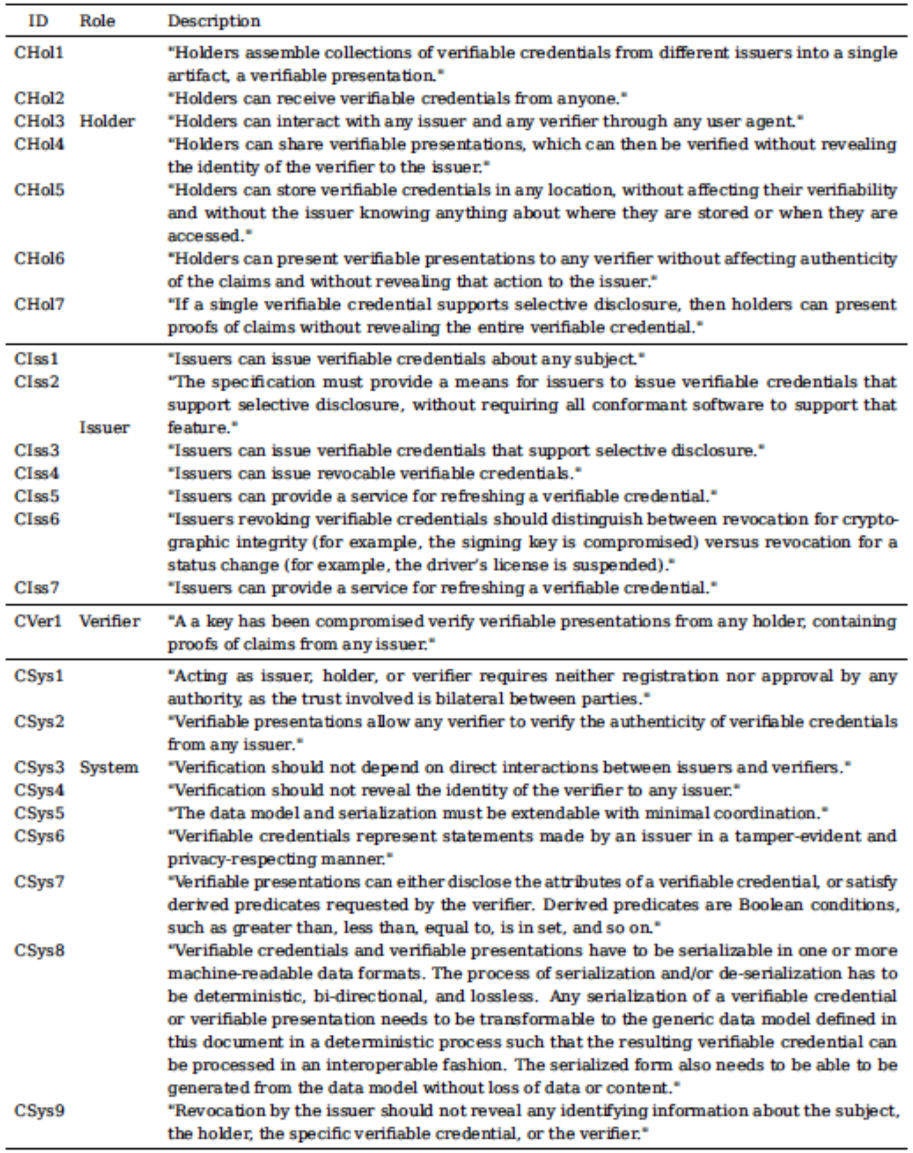
Requirement	Description
Issue	"It MUST be possible for any entity to issue a verifiable credential."
Assert	"It MUST be possible for the holder of a verifiable credential to restrict the amount of information exposed in a credential they choose to share. It also MUST be possible for the holder to limit the duration for which that information is shared."
Verify	"It MUST be possible for a verifier to verify that the credential is an authentic statement of an Issuer's claims about the subject. The verifying entity must have the capability to connect the Issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential. The Issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the Issuer. It MUST be possible to do this in an automated fashion."
Store	"It MUST be possible for the holder of a claim to store that claim in one or more credential repositories."
Move	"It MUST also be possible for the holder to move a claim among credential repositories, and to do so without requesting a new claim from the claim Issuer."
Retrieve	"It MUST be possible for a holder to select if and which appropriate credential should be sent to a verifier."
Revoke	"It MUST be possible for the Issuer of a claim to revoke it, after which it will no longer satisfy verification procedures."

[4]

State of the Art – Characteristics

RQ2

W3C Verifiable Credentials Draft [1]



ID	Role	Description
CHol1	Holder	"Holders assemble collections of verifiable credentials from different issuers into a single artifact, a verifiable presentation."
CHol2		"Holders can receive verifiable credentials from anyone."
CHol3		"Holders can interact with any issuer and any verifier through any user agent."
CHol4		"Holders can share verifiable presentations, which can then be verified without revealing the identity of the verifier to the issuer."
CHol5		"Holders can store verifiable credentials in any location, without affecting their verifiability and without the issuer knowing anything about where they are stored or when they are accessed."
CHol6		"Holders can present verifiable presentations to any verifier without affecting authenticity of the claims and without revealing that action to the issuer."
CHol7		"If a single verifiable credential supports selective disclosure, then holders can present proofs of claims without revealing the entire verifiable credential."
CIss1	Issuer	"Issuers can issue verifiable credentials about any subject."
CIss2		"The specification must provide a means for issuers to issue verifiable credentials that support selective disclosure, without requiring all conformant software to support that feature."
CIss3		"Issuers can issue verifiable credentials that support selective disclosure."
CIss4		"Issuers can issue revocable verifiable credentials."
CIss5		"Issuers can provide a service for refreshing a verifiable credential."
CIss6		"Issuers revoking verifiable credentials should distinguish between revocation for cryptographic integrity (for example, the signing key is compromised) versus revocation for a status change (for example, the driver's license is suspended)."
CIss7		"Issuers can provide a service for refreshing a verifiable credential."
CVer1	Verifier	"A a key has been compromised verify verifiable presentations from any holder, containing proofs of claims from any issuer."
CSys1	System	"Acting as issuer, holder, or verifier requires neither registration nor approval by any authority, as the trust involved is bilateral between parties."
CSys2		"Verifiable presentations allow any verifier to verify the authenticity of verifiable credentials from any issuer."
CSys3		"Verification should not depend on direct interactions between issuers and verifiers."
CSys4		"Verification should not reveal the identity of the verifier to any issuer."
CSys5		"The data model and serialization must be extendable with minimal coordination."
CSys6		"Verifiable credentials represent statements made by an issuer in a tamper-evident and privacy-respecting manner."
CSys7		"Verifiable presentations can either disclose the attributes of a verifiable credential, or satisfy derived predicates requested by the verifier. Derived predicates are Boolean conditions, such as greater than, less than, equal to, is in set, and so on."
CSys8		"Verifiable credentials and verifiable presentations have to be serializable in one or more machine-readable data formats. The process of serialization and/or de-serialization has to be deterministic, bi-directional, and lossless. Any serialization of a verifiable credential or verifiable presentation needs to be transformable to the generic data model defined in this document in a deterministic process such that the resulting verifiable credential can be processed in an interoperable fashion. The serialized form also needs to be able to be generated from the data model without loss of data or content."
CSys9		"Revocation by the issuer should not reveal any identifying information about the subject, the holder, the specific verifiable credential, or the verifier."

Framework

[4]

State of the Art – Technical Analysis

RQ2

```
{
        "@context": [
                "https://www.w3.org/2018/credentials/v1",
                "https://www.w3.org/2018/credentials/examples/v1"
        ],
        "id": "http://tum.de/credentials/3732",
        "type": ["VerifiableCredential", "UniversityEnrollment"],
        "issuer": "https://tum.de",
        "issuanceDate": "2020-04-01T10:09:59Z",
        "expirationDate": "2020-09-30T23:59:59Z",
        "refreshService": {
                "id": "https://tum.de/refresh/3732",
                "type": "StudentIdRefreshService"
        },
        "credentialSubject": {
                "id": "did:tum:ebfeb1f712ebc6f1c276e12ec21",
                "studentEnrollment": {
                        "id": "did:gerbershagen:abcd1f712ebc6f1c276e12ec21",
                        "name": "Dominik Gerbershagen",
                        "studyProgram": "Master of Science Information Systems",
                        "semester": 6
                }
        },
        "proof": {
                "type": "RsaSignature2018",
                "created": "2019-06-10T10:09:59Z",
                "proofPurpose": "assertionMethod",
                "verificationMethod": "https://tum.de/credAssertion/keys/1",
                "jws": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOls"
        }
}
```

W3C Verifiable Credentials Draft – Example Credential with Refreshment Service [1].

Extensibility and Interoperability

Basic credential data

Automatic refreshment of Credential

Information about the subject that is credentialed

Embedded Proof to automatically verify authenticity and integrity of the credential

State of the Art – Technical Analysis

RQ2

```
{               "@context": "https://w3id.org/openbadges/v2",
                "id": "https://tum.de/assertions/241010",
                "type": "Assertion",
                "recipient": {
                                "type": "email",
                                "identity": "dominik@emailaddress.com",
                                "hashed": false
                },
                "issuedOn": "2020-03-15T23:59:59+00:00",
                "verification": {
                                "type": "hosted"
                },
                "badge": {
                                "type": "BadgeClass",
                                "id": "https://tum.de/badges/255",
                                "name": "Blockchain BootCamp",
                                "description": "This badge is awarded for participating in the Blockchain BootCamp",
                                "image": "https://tum.de/badges/255/image",
                                "criteria": {
                                                "narrative": "Students learn the technical foundations about
Blockchain Networks."
                                },
                                "issuer": {
                                                "id": "https://tum.de/issuer",
                                                "type": "Profile",
                                                "name": "Technical University of Munich",
                                                "url": "https://tum.de",
                                                "telephone": "+49089111222",
                                                "email": "contact@tum.de",
                                                "description": "TUM is one of Europe's leading Universities.",
                                                "publicKey": "SHA256:xyz,
                                                "verification": {
                                                                "allowedOrigins": "tum.de"
                                                }}}}
```

IMS OpenBadges– Basic Example Badge [2].

Extensibility and Interoperability

Information about the subject that is credentialed (Only Email)

Verification method is normally set to “hosted”

Credential data

Issuer data

State of the Art – Technical Analysis

RQ2

```
{
  "id": "2018091259",
  "name": "Master of Information Systems",
  "issuedOn": "2020-03-15T23:59:32+08:00",

"issuers": [{
    "name": "Technical University of Munich",
    "url": "https://tum.de",
    "certificateStore": "0x1989a05B320186f5fAc590fFf64730FC9099Bc7b",
    "did": "did:tum:21234567890",
    "email": "certificates@tum.de",
    "phone": "+4908912345678"
  }],

  "recipient": {
    "name": "Dominik Gerbershagen",
    "email": "dominik@mail.com",
    "phone": "+4908965431",
    "did": "did:gerbershagen:123456789"
  },
  "transcript": [{
      "name": "Master Thesis Digital Credentialing",
      "grade": "undefined",
      "courseCredit": 30,
      "courseCode": "MA-DC",
      "url": "https://in.tum.de/masterthesis",
      "description": "State of the art and practice of digital credentialing.",
      "score": 120
    }],
  "additionalData": {
    "signature": "data:image/jpeg;base64...."
  }
}
```

Identification of Credential

Issuer Data

Holder Data

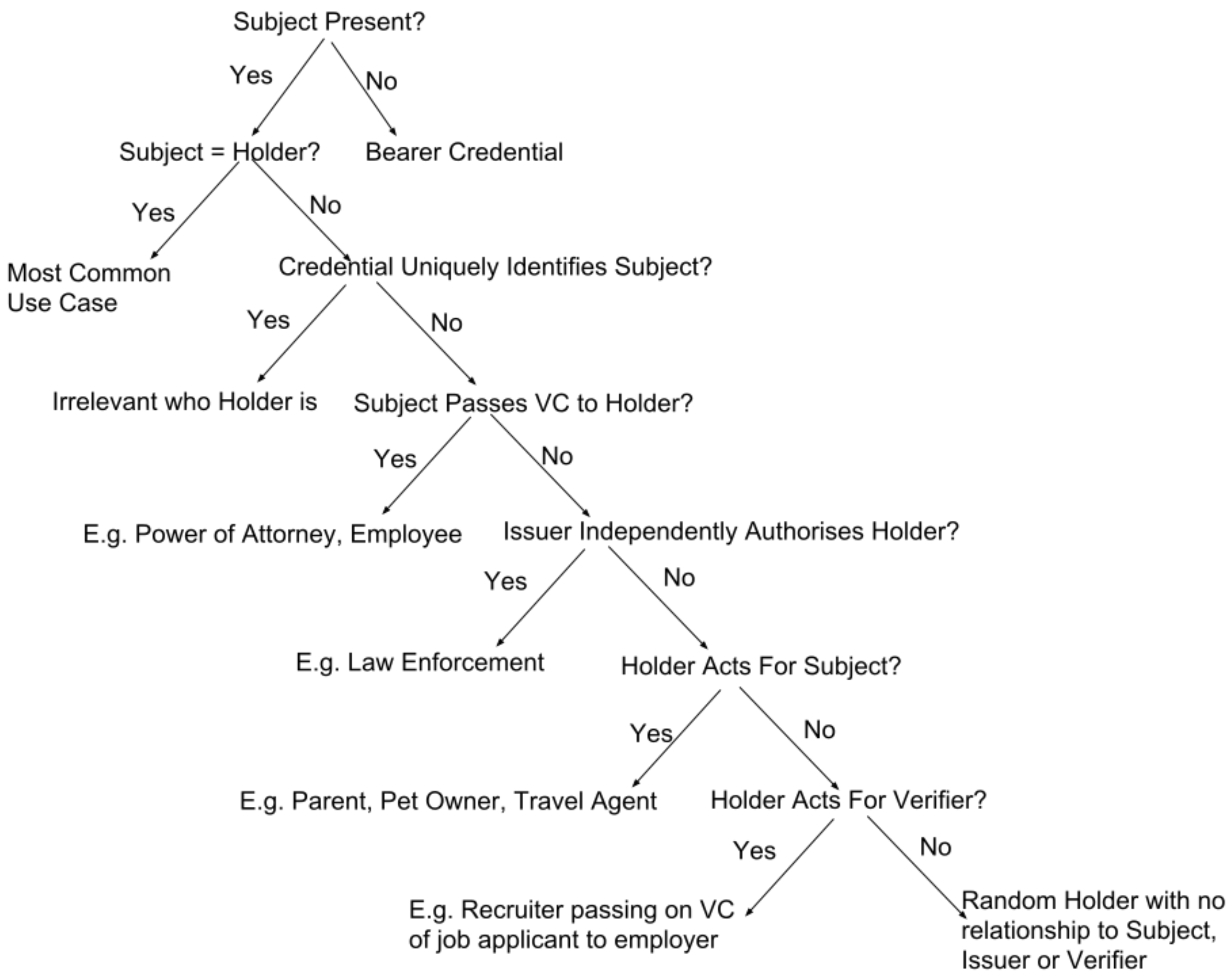
Credential Data

Additional data such as a picture for Micro-Credentials

IMS OpenBadges– Basic Example Badge [2].

State of the Art – VC Holder Model

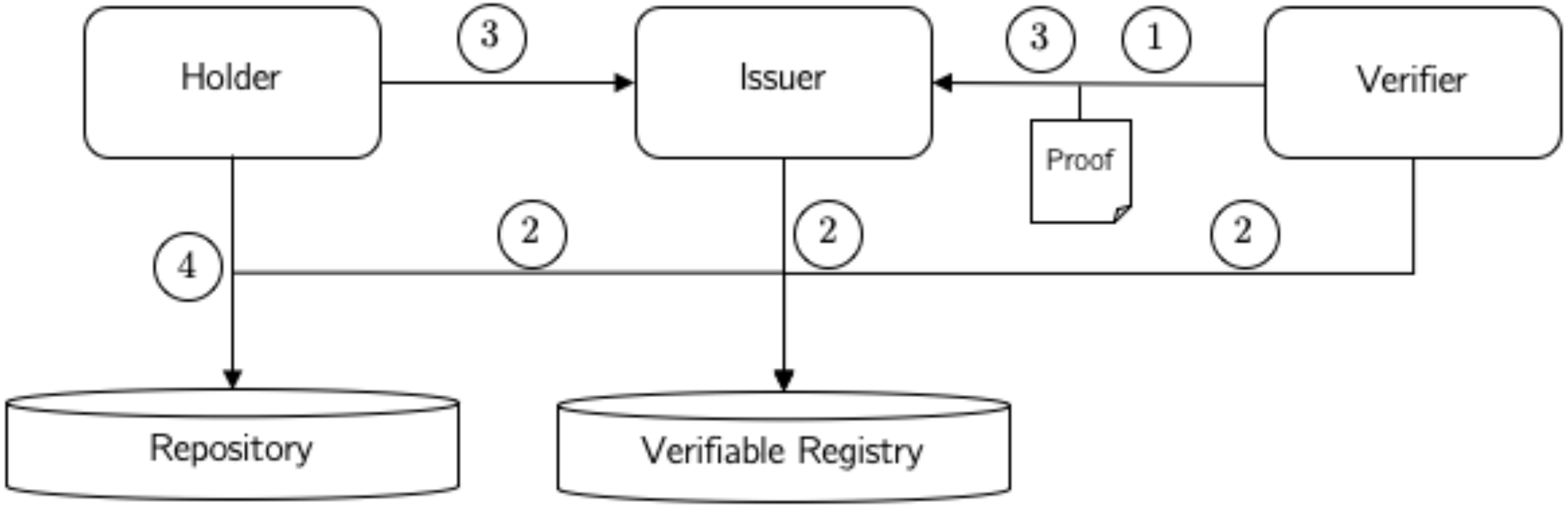
RQ2


Subject Present?
Yes
No
Subject = Holder?
Bearer Credential
Yes
No
Most Common Use Case
Credential Uniquely Identifies Subject?
Yes
No
Irrelevant who Holder is
Subject Passes VC to Holder?
Yes
No
E.g. Power of Attorney, Employee
Issuer Independently Authorises Holder?
Yes
No
E.g. Law Enforcement
Holder Acts For Subject?
Yes
No
E.g. Parent, Pet Owner, Travel Agent
Holder Acts For Verifier?
Yes
No
E.g. Recruiter passing on VC of job applicant to employer
Random Holder with no relationship to Subject, Issuer or Verifier

[1]

State of the Art – Trust Model

RQ2

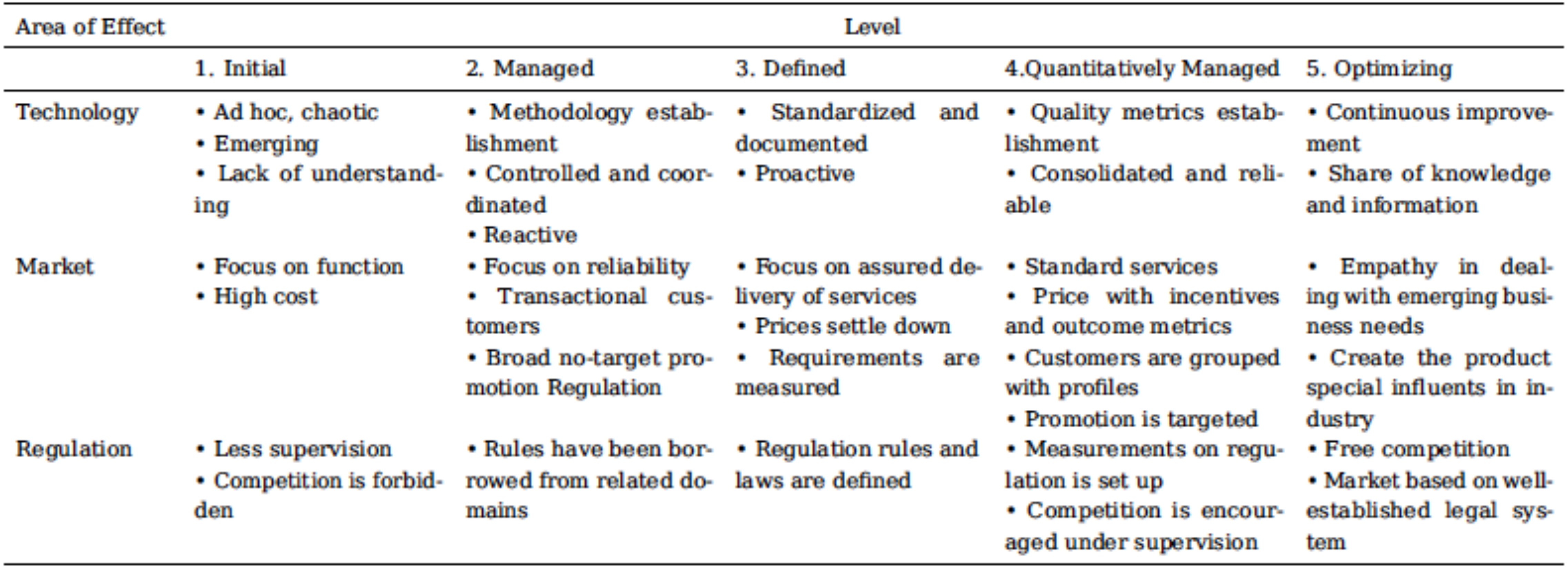


1) Verifier trusts issuer either by proof or tamper-resistant transmission
2) All trust verifiable registry
3) Holder and Verifier trust Issuer to publish correct information
4) Holder trusts the repository (e.g. a Wallet)

[1]

State of the Art – Maturity Model

RQ2



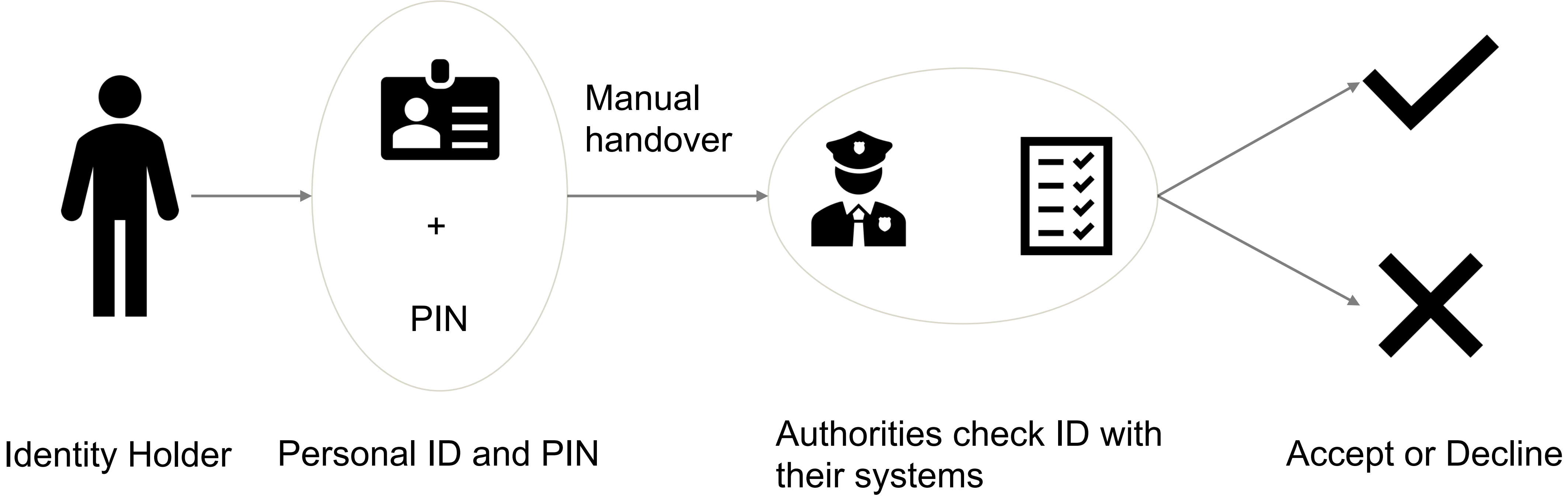
Area of Effect	Level				
	1. Initial	2. Managed	3. Defined	4.Quantitatively Managed	5. Optimizing
Technology	• Ad hoc, chaotic • Emerging • Lack of understanding	• Methodology establishment • Controlled and coordinated • Reactive	• Standardized and documented • Proactive	• Quality metrics establishment • Consolidated and reliable	• Continuous improvement • Share of knowledge and information
Market	• Focus on function • High cost	• Focus on reliability • Transactional customers • Broad no-target promotion Regulation	• Focus on assured delivery of services • Prices settle down • Requirements are measured	• Standard services • Price with incentives and outcome metrics • Customers are grouped with profiles • Promotion is targeted	• Empathy in dealing with emerging business needs • Create the product special influents in industry
Regulation	• Less supervision • Competition is forbidden	• Rules have been borrowed from related domains	• Regulation rules and laws are defined	• Measurements on regulation is set up • Competition is encouraged under supervision	• Free competition • Market based on well-established legal system

[6]

Identification Methods - eIDAS

RQ2

Identification “without permanent proof“ [7]: Traditional approach.



+

PIN

Manual handover

Identity Holder

Personal ID and PIN

Authorities check ID with their systems

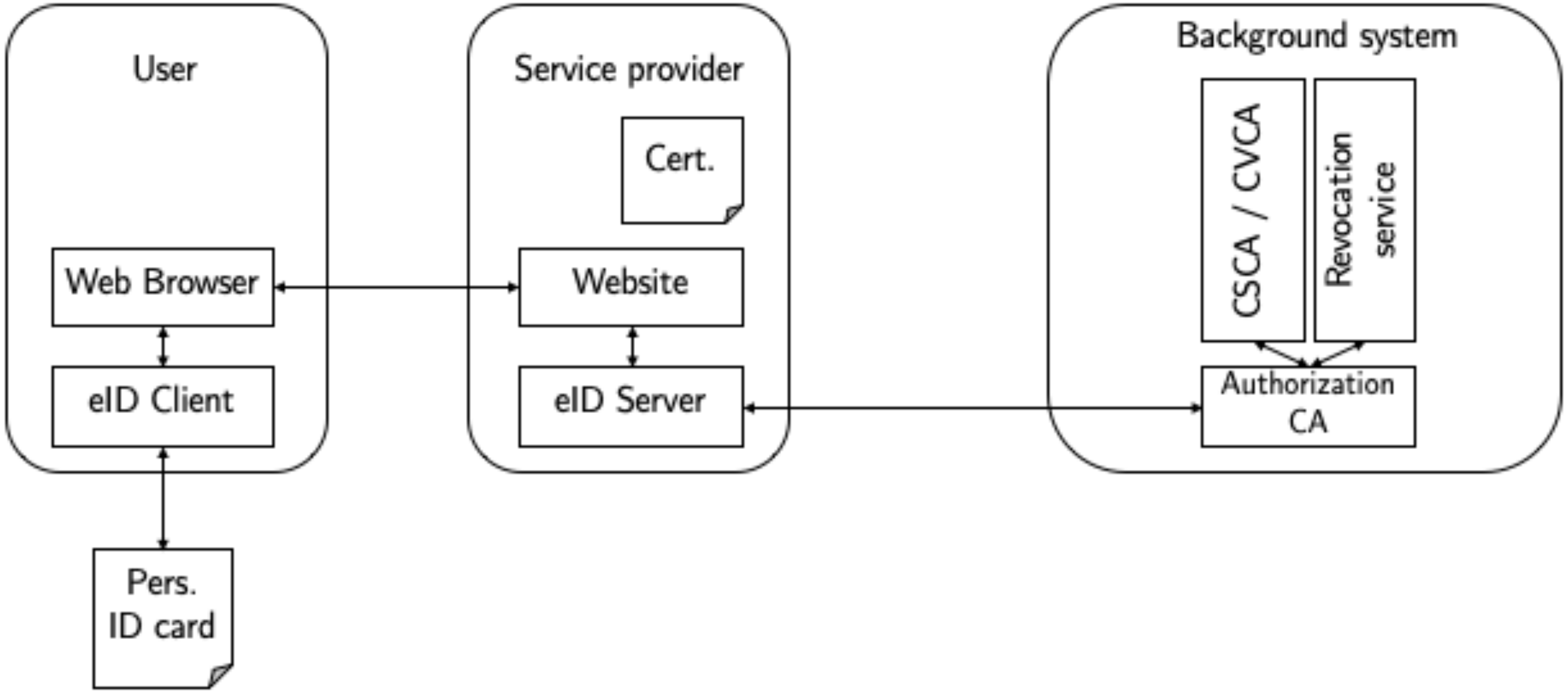
Accept or Decline

[7]

Identification Methods - eIDAS

RQ2

Identification “without permanent proof“ [7]: Translation into the digital realm.

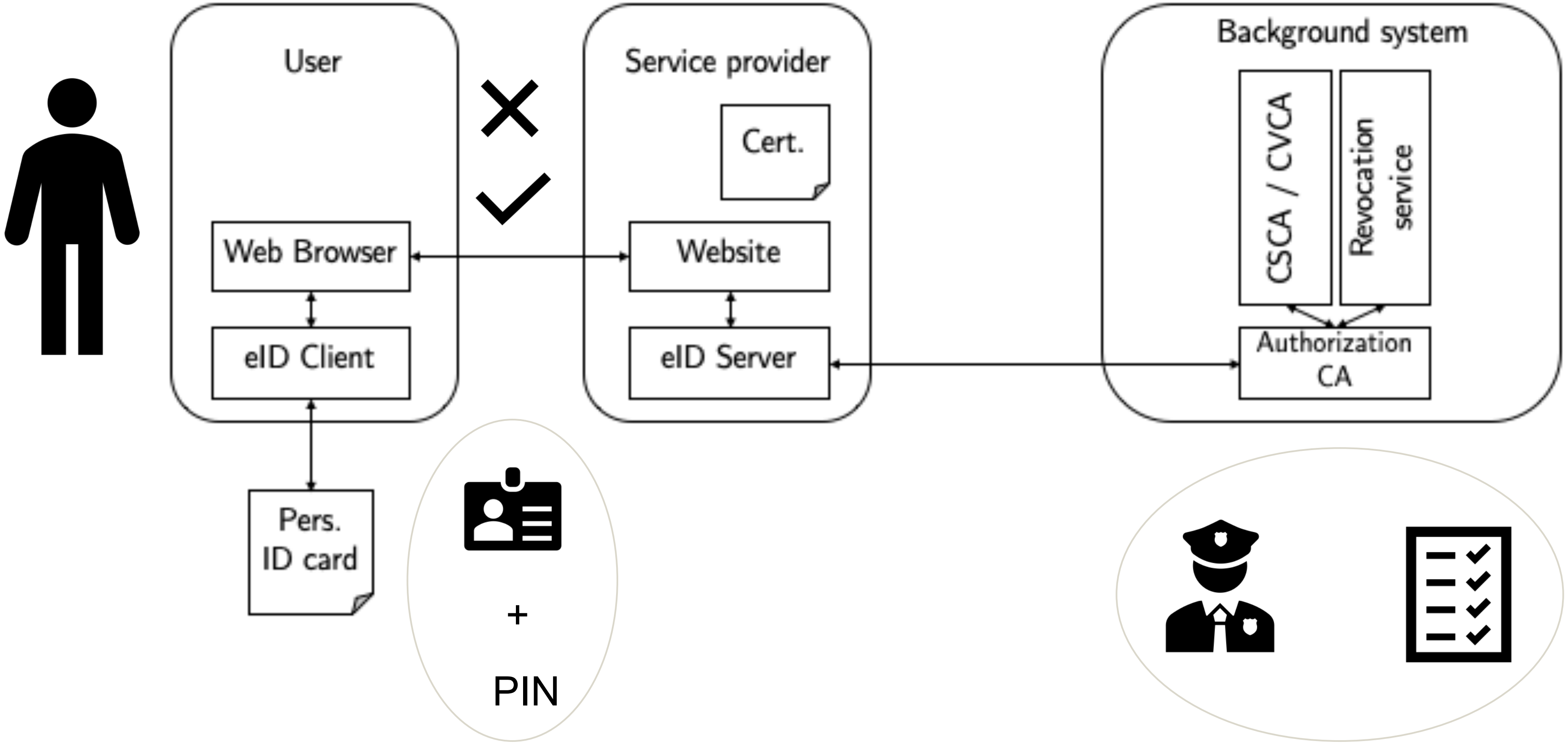


[7]

Identification Methods - eIDAS

RQ2

Identification “without permanent proof“ [7]: Merging both worlds.

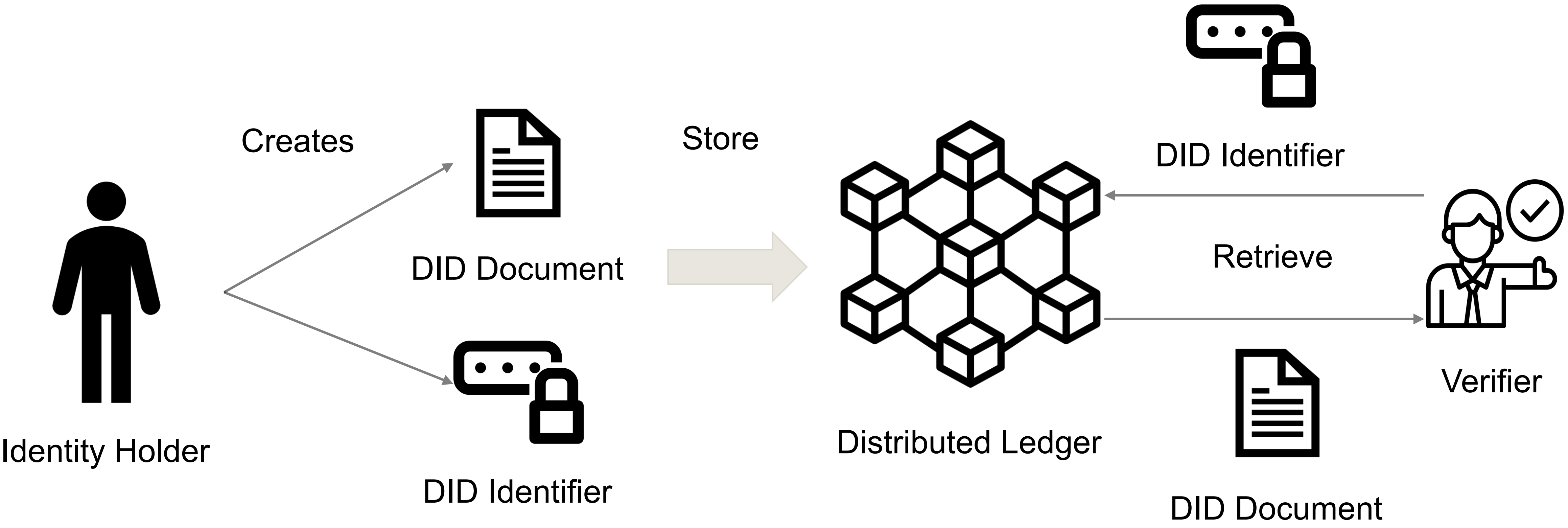


[7]

Identification Methods - DID

RQ2

Fully decentralized identification based on Distributed Ledger technology [8]



[8, 9]

Identification Methods - DID

RQ2

Fully decentralized identification based on Distributed Ledger technology [8]

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{

    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{

    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

DID Document

DID Identifier

did:example:123456789abcdefghi

[8]

List of Investigated Companies and Research Projects

RQ3

- Accredible [101]
- APPII [102]
- BCDiploma [103]
- BlockCo [104]
- BlockCerts [105]
- Blockeducate [106]
- CHESICC [107]
- Credly [108]
- CVTrust [109]
- Edgecoin [110]
- Gradbase [111]
- Sproof [112]
- Keeex [113]
- Parchment [118]
- SAP TrueRec [114]
- Sony GED [115]
- Stampery [116]
- Vottun [117]

- Blockchain and Smart Contracts for Digital Certificates [201]
- Blockchain Education Platform [202]
- Blockchain-Based Education Records [203]
- Blockchain-Based Educational Record Repository [204]
- Blueprint for Learning Trace Repositories [205]
- Certificate Verifyin Support System [206]
- CredenceLedger [207]
- Distributed Credit Transfer [208]
- Educational Certificate Blockchain [209]
- QualiChain [210]

Sources for Companies and Projects

RQ3

- 101 Accredible. Accredible Credential API · Apiary. URL: https://accrediblecredentialapi.
- docs.apiary.io/#.
- 102 APPII. World’s first blockchain career verification platform | APPII. 2018. URL:
- https://appii.io/.
- 103 BCDiploma. BCDiploma White Paper v. 2.2. Tech. rep. BCDiploma, 2018. URL: https:
- //www.evidenz.io/img/pdf/BCD-WhitePaper_last.pdf.
- 104 Blockco. Block.co. URL: https://block.co/.
- 105 Blockcerts. Introduction - Blockcerts : The Open Standard for Blockchain Credentials.
- URL: https://www.blockcerts.org/%20https://www.blockcerts.org/
- guide/.
- 106 Blockeducate. Blockchain For Education, Blockchain Academic Certificate. URL:
- https://blockeducate.com/services/blockchain-for-education/.
- 107 CHISECC. Brief Introduction to Online Verification Report_CHESICC. URL: https:
- //www.chsi.com.cn/xlcx/en/brief.jsp.
- 108 Credly. How Credly Works. URL: https://info.credly.com/how-credly-works.
- 109 CVTrust. Smart Certificate for the education world. URL: https://www.cvtrust.
- com/default.aspx.
- 110 Edgecoin. Edgecoin.io | Fraud-proof, Smart Education on the Blockchain. URL:
- https://www.edgecoin.io/.
- 111 Gradbase. Gradbase - Instantly Verify Qualifications. URL: https://gradba.se/en/
- %20https://www.gradba.se/en/.
- 112 Keeex. Solutions - KeeeX - the Universal Probative Value. URL: https://keeex.me/
- solutions/.
- 113 SAP. TrueRec: digitale Brieftasche mittels Blockchain. URL: https://news.sap.
- com/germany/2017/09/truerec-blockchain/.
- 114 Sony Global Education. SGE Education Blockchain. URL: https://blockchain.
- sonyged.com/.
- 115 Sproof. Schema—sproof 1.0 documentation. URL: https://sproof-docs.readthedocs.
- io/en/latest/schema.html#document.
- 116 Stampery. Stampery Features | Stampery. URL: https://stampery.com/features/
- #existence.
- 117 Vottun. Credentials - Vottun. URL: https://vottun.com/services/digital-credentials/.
- 118 Parchment. URL: https://www.parchment.com/

[201] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen. “Blockchain and smart contract for digital certificate”. In: 2018 IEEE international conference on applied system invention (ICASI). IEEE. 2018, pp. 1046–1051.

[202] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. F. Torres, and F. Wendland. “Blockchain for Education: Lifelong Learning Passport”. In: Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies. 10. European Society for Socially Embedded Technologies (EUSSET). 2018, pp. 1–8. DOI: 10 . 18420 / blockchain2018. URL: https : / / dl . eusset.eu/bitstream/20.500.12015/3157/1/blockchain2018_10.pdf%0Ahttps: //www.fim-rc.de/Paperbibliothek/Veroeffentlicht/756/wi-756.pdf.

[203] M. Han, D. Wu, Z. Li, Y. Xie, J. S. He, and A. Baba. “A novel blockchain-based education records verification solution”. In: SIGITE 2018 - Proceedings of the 19th Annual SIG Conference on Information Technology Education. Vol. 18. ACM, 2018, pp. 178–183. ISBN: 9781450359542. DOI: 10.1145/3241815.3241870. URL: https: //doi.org/10.1145/3241815.3241870.

[204] E. Bessa and J. Martins. A Blockchain-based Educational Record Repository To cite this version : HAL Id : hal-02085749 A Blockchain-based Educational Record Repository. Tech. rep. 2019, pp. 1–11. URL: https://hal.archives-ouvertes.fr/hal-02085749.

[205] J. C. Farah, A. Vozniuk, M. J. Rodriguez-Triana, and D. Gillet. “A blueprint for a blockchain-based architecture to power a distributed network of tamper-evident learning trace repositories”. In: Proceedings - IEEE 18th International Conference on Advanced Learning Technologies, ICALT 2018. Institute of Electrical and Electronics Engineers Inc., Aug. 2018, pp. 218–222. ISBN: 9781538660492. DOI: 10. 1109/ICALT.2018.00059.

[206] D. H. Nguyen, D. N. Nguyen-Duc, N. Huynh-Tuong, and H. A. Pham. “CVSS: A blockchainized certificate verifying support system”. In: ACM International Conference Proceeding Series. 2018, pp. 436–442. ISBN: 9781450365390. DOI: 10.1145/ 3287921.3287968. URL: https://doi.org/10.1145/3287921..

[207] R. Arenas and P. Fernandez. “CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials”. In: 2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings. Institute of Electrical and Electronics Engineers Inc., Aug. 2018. ISBN: 9781538614693. DOI: 10.1109/ICE.2018.8436324.

- [208] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash, and R. Pradhan. “A Distributed Credit Transfer Educational Framework based on Blockchain”. In: Proceedings - 2018 2nd International Conference on Advances in Computing, Control and Communication Technology, IAC3T 2018. Institute of Electrical and Electronics Engineers Inc., Mar. 2019, pp. 54–59. ISBN: 9781538641460. DOI: 10.1109/IAC3T. 2018.8674023.

- [209] Y. Xu, S. Zhao, L. Kong, Y. Zheng, S. Zhang, and Q. Li. “ECBC: A high performance educational certificate blockchain with efficient query”. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. 10580 LNCS. Springer Verlag, 2017,

[210] N. Chowdhury, A. Third, A. Mehrbod, V. Karakolis, C. Kontzinos, C. Botsikas, S. Scerri, I. Keck, N. Politou, and Miguel Correia. D5.1 QualiChain Integrated Architecture. Tech. rep. 2019.