

ENHANCING TRUST IN EMPLOYMENT VERIFICATION THROUGH SELF-SOVEREIGN IDENTITY AND DISTRIBUTED LEDGER TECHNOLOGY

ROBERT OUKO OTIENO

Department of Electronic Systems, Aalborg University, Denmark
A.C Meyers Vænge 15, 2450 København

June 4, 2025



**AALBORG
UNIVERSITET**



Aalborg University

Department of Electronic Systems

<https://www.es.aau.dk>

Abstract:

Title:

Enhancing Trust In Employment Verification
Through Self-Sovereign Identities and
Distributed Ledger Technology

Theme:

MASTERS THESIS

Project Period:

2024-09-01 To 2025-05-31

Member:

ROBERT OUKO OTIENO

Supervisor:

Henning Olesen

Date Of Completion:

June 4, 2025

This project explores the design and implementation of a decentralized employment verification system using Self-Sovereign Identity (SSI) and Distributed Ledger Technologies (DLT). Traditional CVs and employment verification processes often rely on unverifiable, self-asserted claims and institution-bound document checks, resulting in inefficiencies and trust gaps. By analyzing the structure of CVs and associated employment artifacts, this study identifies which elements can be transformed into Verifiable Credentials (VCs) and defines a trust model that distinguishes between high-trust and low-trust issuers. Leveraging technologies such as DIDs, digital wallets, and cryptographic proofs, the system aims to support partial automation of the hiring process while enhancing privacy, authenticity, and cross-border interoperability. The resulting design provides a scalable framework for secure, user-controlled credential exchange across diverse employment contexts.

Contents

1	INTRODUCTION	1
1.1	CURRENT EMPLOYMENT PROCESS	2
1.2	CHALLENGES OF THE CURRENT PROCESS	3
1.3	DIGITAL ENABLING TECHNOLOGIES	4
1.4	PROBLEM STATEMENT	5
1.5	GENERAL OBJECTIVE	7
1.5.1	SPECIFIC OBJECTIVE	7
1.6	SCOPE	7
1.7	OUT-OF-SCOPE CONSIDERATIONS	8
1.8	MOTIVATION	8
1.9	CONTRIBUTION	9
1.10	EXPECTED OUTCOME	9
2	METHODOLOGY	10
2.0.1	Design Science Methodology	10
2.0.2	Deductive Reasoning methodology	10
2.0.3	Realism Methodology	11
2.0.4	Exploratory methods	11
3	EMPLOYMENT PROCESS & VERIFICATION: Contextual and Theoretical Exposition	12
3.1	THE HIRING PROCESS	13
3.1.1	Identify The Hiring Need and Planning	13
3.1.2	Job Design and Description	13
3.1.3	Advertisement and Recruitment	14
3.1.4	Screening and Verification	14
3.1.5	On-boarding and Integration	15
3.2	APPLICATION PROCESS AND SUBMISSION	15
3.2.1	Resume and Application document Requirements	16
3.2.2	Application Documents Preparation Process	19
3.3	INDUSTRY SPECIFIC EMPLOYMENT REQUIREMENTS	20
3.3.1	Health care and Finance	21
3.3.2	Police and Military Recruitment	22
3.3.3	Academia	23
3.3.4	Remote Works	24
3.4	CV STRUCTURE AND ITS COMPONENTS	25
3.5	Barriers and Challenges in the Process	27
4	TRUST IN EMPLOYMENT VERIFICATION;The Evolution from Traditional to Digital Paradigms	28
4.1	Importance Of Trust In Employment Verification	29
4.2	Identity Proofing in Employment Verification	30
4.3	Trust Models in Employment Verification	31
4.4	Evolution of the Trust Models	33
4.4.1	Current Employment Trust Models	33
4.4.2	Paradigm Shift; Ecosystems Era	35
4.4.3	Self-Sovereign Identities Ecosystem	36

5	STATE-OF-THE-ART TECHNOLOGIES	39
5.1	Decentralized Identifier (DID)	39
5.1.1	DID Subject	40
5.1.2	DID Document	40
5.1.3	DID Controller	42
5.1.4	DID Resolution, Dereferencing and Method	42
5.2	Verifiable Credentials (VCs)	43
5.2.1	VC cryptographic Proof Process	43
5.2.2	Verifiable Presentation	44
5.3	Digital Wallets	45
5.4	OpenID4VC	46
5.5	JSON-LD	46
5.6	SD-JWT	46
5.7	Git and Git Hub	46
5.8	Postman	47
6	ENABLING ORGANIZATIONS and FRAMEWORKS	48
6.1	World wide Web Consortium Standards	48
6.2	European Blockchain Services Infrastructure	48
6.3	European Digital identity Wallet	49
6.4	Linux Foundation	50
6.5	OpenID Connect Foundation	51
6.6	Walt.id Framework	52
6.7	Internet Engineering Task Force(IEFT)	53
6.8	Trust Over IP Foundation	53
7	ANALYSIS	54
7.1	Mapping CV Components to Verifiable Credentials	54
7.2	Trust Models and Issuer Classification In Employment Verification System.	55
7.2.1	High-Trust Credentials and Qualified Trust Service Provider	56
7.2.2	DID Methods For Legal Entities under the High-level Trust Credentials	59
7.2.3	Low-Trust Credentials and Trusted Issuers	61
7.3	Towards a Credential Ecosystem for Career Mobility	63
7.4	Technical Considerations For The Design of the Employment Verification System	64
7.4.1	Credential Model and Data Elements	64
7.4.2	DID Methods For Verification in the Decentralized Employment System	65
7.4.3	DID Methods for Employers and Organizations(Legal Entities)	66
7.4.4	Credential Status and Lifecycle Management)	68
7.4.5	Verifiable Attestation Management Strategies for Employees/Job Seekers	69
7.4.6	Verifiable Accreditation Management Strategies for Legal Entities	71
7.4.7	Accreditation process for high-trust credentials	71
7.4.8	Key Management and Security	72
7.4.9	Sequence of High-trust Establishment and Credential Flow	73
7.4.10	Revocation Registry	74
7.4.11	Types of Revocation in the Employment verification	76
7.5	Regulations and Legals Consideration Analysis	77
7.5.1	Consent Management	77
7.5.2	User control via digital wallets	77
7.5.3	Data Minimization and Privacy by Design Compliance with GDPR (Art. 5 and Art. 25)	78
7.5.4	Privacy and Pairwise Identifiers	79
7.6	User Scenarios and Use Cases	79

7.6.1	Scenarios	79
7.7	Interoperability and Integration with Existing Systems	81
7.8	Conclusion of the Analysis	82
8	DESIGN	83
8.1	Service architecture	83
8.1.1	Application Layer	83
8.1.2	Service Layer	83
8.1.3	Libraries and Protocol Support	84
8.1.4	Containerization and Deployment	85
8.1.5	External Integrations	85
8.1.6	API Interfaces	86
8.1.7	Technological stack for the Implementation	87
8.2	The Onboarding/ Registration Process for New Issuers	87
8.3	Verifiable Credential architecture for Employment Verifiable Credentials	88
8.4	Interaction Flows	88
8.4.1	Credential Issuance and the binding Process between the employer and the Employee	89
8.4.2	Presentation and Verification Process Flow	89
8.4.3	Revocation/update Flow	91
8.5	Sequence Diagrams	91
8.5.1	The Authentication and registration sequence Employee Wallet	91
8.5.2	How to Onboard an Issuer Sequence Diagram	91
8.6	Security an Privacy Consideration	92
8.6.1	Cryptographic Proof Mechanisms	92
8.6.2	Employee wallet solution for Data storage design	93
8.6.3	Key Management Autonomy After Accreditation	94
8.6.4	DID Documents and verifier Interaction	94
9	IMPLEMENTATION	96
9.1	Web Wallet Application	96
9.1.1	Authentication interface/Sign In	96
9.1.2	The User Profile Interface	97
9.1.3	Credential Management interface	97
9.1.4	DID Management Interface	98
9.1.5	Event Log Interface	98
9.1.6	Key management Operations	99
9.2	Issuer and Verifier Web Portal	100
9.2.1	Issuer portal	100
9.2.2	Verifiable presentation	101
10	DISCUSSIONS	102
11	CONCLUSION	102
12	FUTURE WORKS	103
A	Appendix I	I
A.1	Requirement Specification	I
A.1.1	Functional Requirement Specification	I
A.1.2	Non-Functional Requirements Specifications	III
A.2	Verifiable Credentials non-normative understanding	V

A.2.1	Definitions of Terms	V
A.2.2	Verifiable Credentials Data Model	VI
A.3	Business Analysis	IX
A.3.1	Value Proposition	IX
A.3.2	Stakeholders	X
A.4	Empirical examples of the Credentials in the current employment landscape . . .	XII
B	Appendix II	XV
B.1	TESTING AND DOCUMENTATION	XV
B.1.1	Test Methodology	XV
C	Appendix III	XVII
C.1	Interview Feedbacks	XVII
C.1.1	Meeting Conversation: Insights on Employment verification Thesis Project	XVII
C.1.2	Meeting with People Experience Specialist	XVIII

List of Figures

1	Google Searches annually relating to lying on CV business/impact-cv-fraud-uk-businesses-employers-need-know	1
2	An Example of a CV and its Component	26
3	Example Flow of The current Trust Establishment Model	33
4	Digital Transformation over time source: https://walt.id/white-paper/digital-identity	35
5	This diagram depicts different components that make up the SSI verifiable credential Ecosystem SOURCE: https://www.w3.org/TR/vc-data-model-2.0/	36
6	A simple example of a DID, Source: https://www.w3.org/TR/did-1.0/	40
7	The entries in a DID document, Source: https://www.w3.org/TR/did-1.1/dfn-did-documents	41
8	An Example of a DID Document	41
9	An example depicting a DID Controller Function	42
10	Basic Components of a Verifiable Credential Source: W3C Verifiable credentials	43
11	View of the proof generation Steps, Source: https://www.w3.org/TR/vc-overview/proof-generation-steps-figure	44
12	An Example of Verifiable Presentation show casing the Presentation verification process	44
13	"Digital Identity: Leveraging the SSI Concept to Build Trust" ENISA report, Jan. 2022 https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-SSI-concept-to-build-trust	50
14	EUDI wallet architecture framework Source: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/	57
15	A diagram demonstrating the Issuer Trust Model interaction Source: https://hub.ebsi.eu/get-started/design/trust-chain	58
16	An Example of an did:ebsi DID Method v1 Source: EBSI EXPLAINED	59
17	Multilevel Trust set up flow for roles and permissions within the Ecosystem Inspired by EBSI Multilevel guidelines setup	60
18	A diagram showing hypothesized Flow of the Employment verifiable credentials in the system	63
19	an Example of DID method for Natural Personal	66
20	Accreditation status information storage for verifiable Accreditation Issuers	69
21	Verifiable Attestations Management Strategies for Natural Persons	70
22	Example of the Accreditation process of the Issuer onboarding	72
23	How to establish Trust between the Issuers and Verifiers Diagram Inspired by EBSI	74
24	Caption	81
25	Service Architecture for the design of the Employment Verification	85
26	A diagram showing Employment VC Schema and its components	88
27	Verifiable credential issuance binding the employer and the employee	89
28	Services Interaction during presentation of an Employment verifiable credential	90
29	This shows the authorization into the holder wallet	91
30	Sequential process of the issuer onboarding and Registry operations	92
31	Web wallet User Sign In Interface	96
32	wallet DID interface and management	97
33	Credential storage and management on the employee wallet	98
34	DID methods within the wallet	98
35	Event logs of transaction in the Wallet	99
36	Public private key management in a wallet	100

37	Employment verification issuance User Interface	101
38	Consent and receiving of VC in a digital wallet	101
39	Verifiable presentation of Emloyemnt Credential	101
A1	Verifiable Claim	VI
A2	Embedded Proof Mechanism	VI
A3	VCs JOSE Enveloping	VII
A4	Selective disclosure	VIII
A5	An Example of an issuer recommendation letter	XIII
A7	Requirements as proof of during employment	XIV
A6	Certification Image verifiable in physical state	XIV
A8	Onboarding a User to the Wallet	XV
A9	Credential Issuance Proof	XV
A10	Issuing the Same VC type twice to the same User	XVI
A11	Verifier Service	XVI

List of Tables

1	Mapping of CV Components to Verifiable Credentials	55
3	Table showing the functional requirements of the system	II
5	Non-Functional requirements table	IV
7	Components of Trust Models	V

LIST OF ABBREVIATIONS

WWW world wide web

SSI Self-Sovereign Identities

HR Human Resource

DLT Distributed Ledger Technologies

EU European Union

DSM Design Science Methodology

POC Proof-Of-Concept

DID Decentralized Identifiers

VCs verifiable credentials

URL uniform resource locator

VCDM 2.0 Verifiable Credential Data Model 2.0

GDPR General data protection regulation

SDK software development kit

APIs application programming interface

PoS Proof of Stake

JSON-LD JavaScript Object Notation for Linked Data

SAP System Applications and Products

eIDAS electronic Identification, Authentication and Trust Services

W3C World Wide Web Consortium

VCs Verifiable Credentials

APIs Application Programming Interfaces

JWT JSON Web Tokens

SD-JWT Selective Disclosure JSON Web Token

EBSI European Blockchain Services Infrastructure

EBP European Blockchain Partnership

PoA Proof of Authority

EVM Ethereum Virtual Machine

HCI Human Computer Interaction

ZKPs Zero-Knowledge Proofs

IDP Identity Provider

CAs Certificate Authorities
PKI Public key infrastructure
KYC Know Your Customer
SP Service Providers
IIW Internet Identity Workshop
AI Artificial Intelligence
HCM Human Capital Management
CV Curriculum Vitae
ATS Application Tracking Systems
HRM Human Resource Management
DSM Design Science methodology
ToIP Trust Over IP
CAs Certificate Authorities
NIST National Institute of Standards and Technology
PII Personally Identifiable Information
PID Personal Identification Data
WAAS Wallet-as-a-service
FINRA Financial Industry Regulatory Authority
ESSIF European Self-Sovereign Identity Framework
QTSPS Qualified Trust Service Providers
TAO Trusted Authority Operator
EAA Electronic Attestations of Attributes
QEAAs Qualified Electronic Attestations of Attributes
QES Qualified Electronic Signatures
RDF Resource Description Framework
EUDI European Digital Identity
OIDC4VCI OpenID Connect for VC Issuance
EAA Electronic Attestations of Attributes
QEAA Qualified Electronic Attestations of Attributes
VC-DM Verifiable Data Model v2.0
ESMA The European Securities and Market Authorities

1 INTRODUCTION

Why employment verification? In the rapidly evolving labour market around the world, employment verification has emerged to be more than just a procedural concept. It is a critical element of the hiring process in terms of establishing trust between employers and employees. The hiring process, which involves several key stages, including identifying suitable talent, verification of the accuracy of information claims by job seekers, which are not only crucial for building and maintaining trust between the employer and the employee, but also with other stakeholders in the business.

Employment is no longer merely a contractual agreement; it is perceived as a relationship built on credibility, transparency, and accountability. However, trust is not inherent; it must be continuously verified and reinforced. This necessity underscores the critical role of employment verification in mitigating risks associated with misrepresentation and fraud within the labor market. This raises important questions like how employment verification reinforces trust.

Research highlights the increasing prevalence of credential fraud. For example, according to [116], the increasing pressure to secure jobs often leads candidates to falsify their CV creating significant challenges for organizations. Signalling theory [15] and research by Thomas Hess of Copenhagen Business School [69] suggest that there is information asymmetry between job seekers and employers due to a conflict of interest. Employees seek higher-paying roles, while employers prioritize hiring candidates with the necessary competencies and skills. In the UK, one in ten people admits lying on their CV or knows someone who has done so [83]. In addition to all the above, it has been discovered that 33% of applicants in the UK provide false information, with 40% fabricating academic qualifications and 11% inventing entire degrees [26].

Alarmingly, according to a research survey conducted by CIFAS UK latest 2024, Google records over 26,000 annual searches related to lying on CVs. Figure 1 illustrates the search trends associated with CV fraud, reflecting growing global concerns about why appropriate verification mechanisms must be established.[83].

Rank	CV Deceit Topic	Google Searches March 2022 – February 2023	Google Searches March 2023 – February 2024	% Change
1	Lying on CV	19,120	26,720	39.75%
2	Fake references	7,690	10,040	30.56%
3	Fake qualifications	920	1,200	30.43%
4	CV fraud	1,430	1,540	7.69%
5	Fake work experience	1,230	1,320	7.32%

Figure 1: Google Searches annually relating to lying on CV business/impact-cv-fraud-uk-businesses-employers-need-know

To combat the concerns of trust reinforcement globally, companies have increasingly outsourced employment verification to third-party agencies such as Talio [158] and Workday [157], while some governments, such as Australia, have imposed fines and penalties on individuals caught using fraudulent resumes to deter deception. These efforts in general underscore the critical role of trust and integrity in hiring and the

need to explore the field even further. However, these measures, even though effective, come with some setbacks for example, verification methods used remain costly, inefficient, and prone to manipulation as technologies evolve quite rapidly. And because of these gaps, the need for a more secure, scalable and state-of-the-art solution becomes more apparent.

The rise of decentralised technologies, particularly Self-Sovereign Identities (SSI) and Distributed Ledger Technologies (DLT), presents an opportunity to enhance trust in the hiring process by ensuring a secure, tamper-evident manner of verifying claims and credentials among employers to employers and employers to employees. These technologies not only enhance trust but also promise to automate key stages of the verification process.

Thus, this thesis explores how employment verification processes can be improved through the use of SSI and DLT. By leveraging these technologies, we aim to evaluate which processes in the hiring process can be automated, and how trust can be established between the employer and employee by looking into the current process and enablers.

1.1 CURRENT EMPLOYMENT PROCESS

The hiring process typically begins with an employer recognising the need to fill a position, leading to the development of a job description outlining the required qualifications, responsibilities, and skills for the role [166]. Once the job description is finalised, the vacancy is advertised on various platforms, including company websites, job boards, social networks, and recruitment agencies[21].

The recruitment phase involves identifying and attracting potential candidates, followed by a screening process to evaluate the applicants and filter out those who do not meet the criteria. Screening methods may include resume evaluations, pre-employment evaluations, and applicant tracking systems to streamline candidate selection [27]. The selected candidates are then invited for interviews, where employers further assess their competencies, cultural fit, and suitability for the role[45]. The interview stage can incorporate diverse modalities, such as face-to-face interviews, virtual(online) sessions, or pre-recorded virtual interviews facilitated by AI technologies.

As part of the interview process, employers often conduct employment verification to confirm the accuracy of a candidate's qualifications, professional experience, and other claims made during the application process[155]. This verification step may involve reference checks, credential validation, and background screening, ensuring that only the most qualified individuals proceed to the final stages of recruitment[102]. Usually, the number of interviews varies depending on the organisations hiring policies and complexity of the role, with some roles requiring multiple stages of assessment before a final hiring decision is made.

However, qualification verification does not occur immediately after application submission. Typically, once a candidate successfully passes the interview, employers request official documents such as university transcripts, work experience records, criminal background checks, and professional certifications. These documents are then verified through various methods, including direct communication with issuing institutions, "Phoning Home", emails, or in some cases, physical visits to confirm authenticity[22].

For cross-border and international candidates, the verification process becomes even more complex due to differences in verification standards and procedures across countries. Growing organizations, small and medium enterprises that often lack resources or infrastructure, are particularly challenged in conducting thorough checks. They are

typically forced to rely on third-party agencies for background checks. Once a candidate is selected as the most suitable candidate, a probation period is usually in place to assess their fit within the company culture and environment.

1.2 CHALLENGES OF THE CURRENT PROCESS

Despite advancements in digital records and verification mechanisms, employment verification in the entire process remains a significant challenge. For instance, while digital transformation and national registers have improved the ability to distinguish between authentic and fraudulent credentials, verification is still prone to inconsistencies, data manipulation and identity fraud[68] i.e., digital repositories have helped mitigate some of the risks by providing centralised and verifiable data sources, but yet, discrepancies in candidate qualifications may still go unnoticed [108].

A particularly notable risk is the delayed discovery of falsified experience or academic credentials, often surfacing only after onboarding. This leads to significant financial implications, such as increased training costs, lost productivity, and reputational damage. In some cases, such discrepancies are uncovered months into employment, compounding organizational losses and eroding trust in existing verification procedures.

Traditional verification methods which still heavily rely on manual checks and fragmented data sources, contribute further to inefficiencies and delays in hiring decisions. Historically, Curriculum Vitae (CV) have served as the primary artifact for evaluating candidacy suitability, often supplemented by face-to-face interviews considered the gold standard for assessment[170]. However, empirical evidence suggests that interview scores are not always predictive of job performance. Moreover, recent studies and industry reports have exposed new risks introduced by virtual and asynchronous AI-assisted interviews[39]. These include instances where individuals manipulate the technology using deepfakes, voice spoofing, or paid proxies to attend video interviews on behalf of others. Alarmingly, there have been documented cases where the individual who appears in a video interview is not the same person who reports to work post-hire[87],[72]. Such tactics significantly undermine the reliability of digital interview formats and highlights the urgent need for more robust tamper-proof verification frameworks in recruitment.

The prevalence of credential and identity fraud further reinforces the need for stronger, trustworthy, and secure verification mechanisms in the employment landscape. Applicants falsifying or misrepresenting their qualifications and work experience, with the current verification methods, such as phoning home, emailing, or recommendation letters, this proves insufficiencies in detecting discrepancies as false information can easily bypass these checks, leading to the hiring of unqualified individuals, which ultimately affects organisational efficiency and workforce performance.

With indications of 31% surge in document fraud by 2023 from [4], and the European Commission's 2023 Annual report on Protections of EU's Financial interests at 8% , increases there reported fraud and regulations in EU member states[121]. Further evident data from Sumsub [114] also shows a notable rise in deepfake-related fraud cases in Europe between 2022 and first quarter of 2023, further complicating efforts to verify candidate credentials accurately.

Beyond credential and identity fraud, employment verification domain also faces significant time and cost constraints, impacting both job seekers and employers. Conducting thorough background checks, especially for international hires in

any industry, can be both time-consuming and expensive. Many organizations struggle to allocate the necessary resources for comprehensive candidate verification, leading to either lengthy hiring delays or, in some cases, the decision to bypass verification altogether, putting businesses at risk. Similarly, job seekers face inefficiencies in adapting their resumes to different formats, tailoring competencies to match specific roles, and managing multiple versions of their credentials. This process is not only tedious but also contributes to inconsistencies in how qualifications are presented and evaluated.

However, despite of these challenges, the digital solutions have introduced significant improvements in automating parts of the hiring process. Many organizations now use Application Tracking Systems (ATS) to streamline candidate screening, AI-driven tools for resume analysis, and digital identity verification platforms to enhance security. Additionally, background checks, which once depended on manual verification, are increasingly digitized, offering faster and more scalable identity verification capabilities. Enhance, while automation has improved efficiency in certain aspects, the employment verification process remains fragmented, with varying levels of digitization across industries and regions, and many processes still require manual intervention, leading to inconsistencies, inefficiencies and vulnerabilities. Thus, this raises the question for our project research;

Can all aspects of employment verification landscape be fully automated? and if so, what technologies are best suited to ensure trust, accuracy and compliance in the hiring process?.

1.3 DIGITAL ENABLING TECHNOLOGIES

As outlined in 1.2, the field of Human Resource (HR) has undergone a profound digital transformation over the past few decades, driven by rapid advancements in automation and Human Capital Management (HCM) through Artificial Intelligence (AI), data aggregation and analytics, and identity management technologies [172]. This shift has elevated HR from a traditional administrative function to a strategic enabler of organizational growth, allowing companies to streamline processes and make more data-driven decisions.

One of the most significant advancements driving this transformation is AI-powered recruitment, which has not only streamlined hiring processes but also redefined expectations around data reliability and decision making accuracy. Technologies such as deep Learning, natural language processing, conversational chatbots, gamification and virtual interviews now enable sophisticated automation across resume screening, candidate evaluation, and scheduling [111]. These innovations reduce the reliance on manual process, error-prone workflows, allowing HR professionals to focus on strategic imperatives such as talent development, employee engagement and long-term business goals [59].

Importantly, the successful integration of these tools signals a growing organizational appetite for technologies that can ensure both efficiency and trustworthiness in employment data. This create a fertile ground for embracing more transformative solutions, including systems that not only automate recruitment but also verify the authenticity and integrity of data sources themselves such as verifiable credentials and decentralized identity frameworks. As organizations increasingly recognize the limitations of traditional documentation and self-declared CVs, the appeal of a temper-evident, machine-verifiable employment records becomes both a strategic and operational imperative.

In this emerging digital landscape, Verifiable Credentials (VCs), offer a new paradigm

for expressing and verifying claims such as employment records, academic qualifications, and professional certifications using structured, cryptographically signed data[174]. Unlike the traditional document-based claims VCs can be instantly validated by third parties without needing to contact the original issuer, thereby reducing verification delays and mitigating fraud risks.

Complimenting VCs is the concept of SSI, a decentralized identity model that places individual in full control of their personal information[147]. With SSI, individuals can selectively disclose only the information required for a given verification context empowering privacy-preserving interactions between applicants, employers, and third-party verifiers.

Underlying these innovations is DLT[43], which provides a tamper-evident infrastructure for securely anchoring verification events and credential metadata. Unlike centralized databases, DLT distribute data across a consensus-based network, enhancing transparency, resilience, and auditability essential qualities for cross-border and high-stakes hiring scenarios

In the digital world, VCs, defined as a specific way to express a set of claims made by an issuer, such as a driver's license or an education certificate, provides a structured and cryptographic way to issue, hold and verify credentials such as employment records, diplomas, and certifications. And unlike the traditional documents claims, VCs can be verified instantly without contacting the issuer, reducing delays and fraud risks.

Together, these technologies converge to form a next-generation employment verification ecosystem. Applicants can hold their credentials in digital wallets, which act as secure personal agents that facilitate seamless, consent-driven sharing of verified data. Employers, in turn, can validate credentials in real-time, reducing reliance on manual background checks and inconsistent documentation practices. This shift not only improves operational efficiency but also established a stronger foundation of trust and standardization across industries.

However, important question remain; Can every facet of employment verification be digitized, or do certain components still require human oversight? Which parts of document-based CV claims are most amenable to this digital transformation? And How might organizations move toward a universal model of trustworthy, scalable and privacy-respecting employment verification? These open challenges form the basis for our exploration in this study, setting the stage for a deeper investigation into the technological, procedural, and regulatory dimensions of decentralized employment verification

1.4 PROBLEM STATEMENT

The current employment verification process is fraught with systematic inefficiencies that impede trust, accuracy and operational efficacy. Traditional methods often involving manual checks of seals, stamps and logos, reliance on self-reported CVs, institution-specific documentation, and varied application formats, all with contribute to a verification process that is notably slow, error-prone, and challenging to scale effectively. Research highlights concerns regarding administrative burden especially technical, operational and privacy challenges burdens imposed, exposing hiring organizations to increased risks of credential fraud and misrepresentation, as well as inconsistent assessment standards [85]. The risks are more complicated in the cross-boarder hiring contexts due to diverse legal and regulatory frameworks that vary by jurisdiction. Compliance with data privacy regulations, such as General data protection regulation (GDPR), remains a significant hurdle for traditional systems that

often lack robust mechanisms for consent management and data protection[7].

A major flaw in conventional verification systems is their failure to provide a transparent and reliable method for validating both the origin of credentials and the authenticity of their presenters. Consequently, employers frequently resort to using opaque or unverifiable sources, while applicants often have limited control over the management and sharing of verified records. This imbalance creates a fragile trust environment that hampers the scalability and inclusivity of global hiring frameworks[91]. In essence, the lack of mutual assurance in these systems presents systematic challenges that necessitate innovative solutions.

Emerging Web3 technologies, including SSI, DLT, and W3C VCs, present transformative opportunities for the re-envisioning of employment verification. These technologies offer frameworks for facilitating the cryptographically verifiable, privacy-preserving, and user-controlled exchange of credentials. However, despite the advantages they confer, ambiguity persists regarding which elements of the hiring process could benefit most from automation and decentralization, as well as which specific credential types are most suited for verification within these new paradigms[62]. The absence of comprehensive implementation guidelines and interoperable standards remains a notable barrier to widespread adoption across various sectors.

Nevertheless, the prospect of establishing a decentralized, trust enhancing employment verification system is significant. By capitalizing on SSI and DLT, hiring process could evolve into secure, efficient, and verifiable workflows that maintain individual privacy while also providing institutional assurance. This thesis investigates how a digital trust infrastructure could supplant fragmented, paper-based verification methods. It specifically examines which verifiable employment credentials can be effectively issued and validated within this framework and how these advanced capabilities can address current challenges in global and cross-jurisdictional hiring scenarios.

Research Question:

How can a decentralised trust framework, incorporating SSI and DLT technologies be applied to support the partial automation of employment verification process, particularly in relation to CV data while enhancing trust and efficiency in the hiring process?

Key Issues to the Problem

1. What mechanisms can be used to establish a verifiable trust relationship between the issuer of employment credentials (employers) and the employee in the decentralized identity system?
2. How can the trustworthiness of employee presenting employment credential be established to prevent fraud and ensure the authenticity of information during the verification process?
3. which components of a CV can be effectively represented through Verifiable Credentials improve the accuracy and efficiency of employment verification process.?
4. What role do existing initiatives such as EBSI and Other SSI frameworks play in shaping the adoption of decentralised employment verification

1.5 GENERAL OBJECTIVE

The general objective of this project is to design, demonstrate and evaluate a decentralised employment verification system leveraging SSI, VCs, DIDs and DLT technologies. This system aims to streamline the verification process by enabling secure, efficient, and privacy-preserving interactions between issuer employers, employees, and verifiers, new employers. By addressing the limitations of traditional verification methods, such as inefficiencies, data security risks, and lack of user control, the project seeks to establish a reliable framework that enhances trust, simplifies cross-border verification, and aligns with modern privacy and regulatory standards.

1.5.1 SPECIFIC OBJECTIVE

- **Identify VCs:** To determine which employment-related credentials can be effectively adopted into a digital VC from the CV components
- **Develop a POC:** To design and implement a mini prototype utilising SSI and DLT technologies, demonstrating their feasibility in the employment verification process
- **Evaluate Efficiency:** To assess the efficiency of the proposed solution compared to traditional verification methods, particularly in terms of cost, time and privacy preservation
- **Examine Industry Applicability:** To evaluate the suitability of the solution across different industries, identifying sectors where it can deliver the highest impact in streamlining the hiring process
- **Promote user-centric control:** to empower individuals by enabling them to securely own, manage and share their employment credentials, fostering trust and transparency between employees and employers.

1.6 SCOPE

This project aims to develop a Proof-Of-Concept (POC) for a decentralized verification system rooted in the principles of SSI and utilizing DLT. The initiative emphasizes the formulation and management of verifiable credentials, tailored specifically for employment verification applications within the context of European Union (EU) regulatory frameworks.

in scope elements include:

- **Eu Cross-Border verification Use Case:** The proposed solution evaluates employment verification challenges that transcend EU member states, focusing on enhancing interoperability, trust, and the exchange of credentials within a unified regulatory context, particularly under GDPR and eIDAS regulation. The harmonization of legal frameworks among the EU nations presents an opportunity to prototype cross-border employment verification systems facilitating improved trust through shared regulations
- **Design and Issuance of New Employment Verifiable Credentials:** Central to this project is the conceptualization and design of new verifiable credentials type for employment. This credential will capture structured employment data, including employment history, job roles, duration, and organizational metadata, in a cryptographically verifiable format adhering to the W3C Verifiable Credentials Data Model 2.0.

- **SSI-based Trust Model implementation:** The implementation will delineate roles for three primary stakeholders; issuers (employees), holders (employees) and verifiers (prospective employers). A trust framework will be established based on DIDs and cryptographic proofs.
- **Privacy and Consent Considerations:** To ensure compliance with GDPR mandates related to user consent and data processing, the system will integrate foundational consent management features. This aspect will focus on data minimization, user empowerment and specific data utilization, addressing essential GDPR compliance principles while avoiding an exhaustive legal compliance audit.

1.7 OUT-OF-SCOPE CONSIDERATIONS

Although the project aspires to address the global challenges of employment verification, it is scoped as a POC and thus has defined boundaries. The following aspects are considered out of scope for this project.

- **Global Market Adoption:**
Although the proposed solution offers a globally applicable decentralized employment verification system, the project will not investigate the detailed adoption process in global markets. This is due to the complexities and variations in legal, regulatory, and compliance frameworks across different jurisdictions.
- **Regulatory Compliance Analysis:**
While compliance with privacy laws such as GDPR is acknowledged, an in-depth analysis of regulatory requirements in multiple countries and regions is beyond the scope of this project.
- **Integration with existing HR systems:**
The focus will be on demonstrating the feasibility of a decentralised approach, but the project will not delve into integrating the proposed solution with existing HR platforms.
- **Full-Scale Implementation and Scalability**
The project will not address the broader technical and operational considerations for scaling the system to support large enterprises, multi-industries use cases or a global deployment.
- **Industry-Specific Customisation**
While the solution's potential efficiency across various industries will be evaluated, detailed customisation for specific sectors will not be included.

1.8 MOTIVATION

The motivation for transforming employment verification into a digital process stems from the inefficiencies, inaccuracies and challenges of traditional methods. Current approaches are often labour-intensive, time-consuming and prone to errors, particularly in verifying claims from credentials like education, skills and proof of employment history across borders[152]. Issues like document falsification, delays and inconsistencies hinder hiring processes, negatively impacting both candidates and employers. With the increasing demand for the global workforce and seamless onboarding, there is a pressing need for systems that are efficient, scalable and trustworthy.

By leveraging SSI and DLT with inspiration drawn from European Blockchain Services Infrastructure (EBSI), the importance of this transformation becomes more evident. These technologies enable the creation of Verifiable Credentials, allowing candidates to securely and selectively share authenticated data with employers[16]. This not only reduces the risk of fraud but also ensures data privacy and compliance with regulations like GDPR. The ability to streamline and automate verification processes improves hiring workflows, reduces costs, and enhances the candidates' experience. Additionally, digital verification aligns with the global trend of digitisation and provides a foundation for trust, transparency, and efficiency in the ever-evolving employment landscape

1.9 CONTRIBUTION

This research contributes to the academic investigation of employment by exploring existing research and technological landscape in collaboration with a company, it includes research initiatives by established institutions and organisations like EBSI and Trace4eu which have projects like document traceability. It examines which credentials are most likely to be digitised in the hiring process, focusing on high-trust industries.

Additionally, the research highlights the role of VCs and Selective Disclosure as established methods for secure and privacy-preserving verification, rather than introducing them as new concepts. By addressing gaps in current practices, this work aims to advance understanding, propose scalable solutions and provide insights into the adoption of SSI and DLT in modern employment verification systems.

1.10 EXPECTED OUTCOME

The presumed outcome of this project is to validate the feasibility and transformative potential of a decentralized employment verification system using SSI and DLT technologies. A key deliverable is a functional prototype for the proof-of-concept that demonstrates the core processes of issuing, managing, and verifying employment credentials within a decentralized framework. This system is expected to improve efficiency by simplifying and accelerating verification workflows, reducing time, cost, and manual effort compared to traditional methods. Furthermore, the project aims to establish improved trust and transparency by using tamper-resistant, decentralized mechanisms that empower employees with control over their credentials while ensuring secure and reliable verification for employers. Privacy preservation will be a critical aspect, ensuring that personal data is shared only when necessary and under the control of the employee. The project will also assess the solution's potential applicability in cross-border verification scenarios, providing insights into the opportunities and challenges posed by diverse regulatory environments. Furthermore, an evaluation of industry-specific efficiency gains will identify sectors that stand to benefit most from decentralised employment verification. Finally, the findings are anticipated to inform future research, offering recommendations for scaling the solution, integrating with existing HR systems, addressing legal and regulatory hurdles, and tailoring it to industry-specific needs, thus paving the way for real-world adoption.

2 METHODOLOGY

This chapter is set to outline the research design, methods and procedures used to explore and validate the feasibility of this thesis. Given the project’s aim of enhancing trust, privacy and efficiency in employment verification processes, it details the systematic approach taken to collect, analyse and interpret data relevant to developing a robust POC system. We employ a multi-methodological reach approach to systematically develop, evaluate and analyse the implementation of SSI-based employment verification system with the aid of DLT. Given how complex employment verification can become with all the technological, regulatory and organisational factors intersecting, we integrate design science, deductive reasoning, positivism, and realism to ensure methodological rigour and practical relevance of the project.

we particularly use Design Science methodology (DSM) to provide a structured framework for developing and evaluating technological artefacts, ensuring that the proposed POC system effectively addresses privacy, security and efficiency challenges [80]. Deductive reasoning is employed to derive hypotheses and expositions from existing theoretical frameworks, allowing for systematic hypothesis testing and validation [162]. while Positivism, rooted in the work of [169]; [31], ensures empirical rigour through the collection and statistical analysis of quantifiable metrics, such as fraud reduction and system adoption. Finally, we use Realism [5] as is incorporated to explore underlying socio-technical mechanisms, providing a deeper understanding of the conditions that influence the effectiveness and adoption of the employment verification systems.

By integrating these methodologies, this research project ensures both scientific validity and practical applicability. The combination of design, empirical validation, hypothesis testing and socio-technical analysis enables comprehensive evaluations into the potential of SSI and DLT to transform employment verification processes.

2.0.1 Design Science Methodology

For the success of this project, we adopt DSM in the efforts to develop a Prototype for a decentralized employment verification system using SSI and DLT. DSM is particularly suited for research that seeks to create and evaluate innovative artefacts to address real-world problems [80]. In our use case, the artefact is a trust-based Employment verifiable credential that enhances the trust between the employer and employee by leveraging technologies such as EBSI, VCs, and DIDs. Following the DSM principles, we first identify gaps in the current employment frameworks in verification, and its requirements [129]. The system is then designed with a Trust Over IP (ToIP) architecture, incorporating issuer, holder, and verifier interactions. Through the interactive prototyping and evaluation, the research ensures that the developed solution aligns with the security, compliance, and usability requirements [75]. The final system will be validated through real-world application and stakeholder feedback, demonstrating the practical utility of design science in identity management and employment verification

2.0.2 Deductive Reasoning methodology

Deductive reasoning is a logical, hypothesis-driven research approach that begins with a general theory or principles, which is then tested through empirical observations [162]. It follows a top-down structure, where broad theoretical concepts are systematically refined into specific hypotheses and tested using real-world data [96].

This project applies the approach grounded in the structure of traditional CVs, common hiring practices, and industry-specific employment requirements. Beginning with the premise that existing CV components represent self-asserted claims often requiring manual verification, the study draws on the established principles from SSI and DLT technologies to hypothesize that certain elements such as employment history, academic qualifications and professional certifications can be more reliably and efficiently represented through verifiable credentials. These hypotheses inform the design of our decentralized employment verification system that aligns with real-world hiring workflows and sector-specific recruitment standards. The evaluation framework thus measures the impact of VC substitution on trust, efficiency and alignment with industry expectations, validating or refining the theoretical model accordingly.

2.0.3 Realism Methodology

This research quest also adopts a critical realist philosophical stance to examine how decentralized identity technologies can improve employment verification process. Acknowledging that employment practices, trust relationships, and credentialing systems are rooted in real structures, the study investigates the casual mechanisms through which verifiable credentials and SSI frameworks might enhance accuracy and efficiencies in CV verification[5]. However, outcomes are understood to be context-dependent, shaped by industry specific norms, regulatory settings, and organizational workflows. This perspective informs both the design of the proposed solution and the evaluation of its impact through mixed methods i.e system demonstration, scenarios-based walk-through, and qualitative analysis, focusing on the relationship between technological artifacts and their embedding social contexts[144].

The reason being, no single data collection method is always ideal as each of them has inherent strengths and weaknesses. We enhance the reality of our findings by triangulating findings from various sources. Interview data from different experts with HR and IAM teams in collaboration in a company. These findings are well documented in efforts to streamline the analysis of the project.

2.0.4 Exploratory methods

We finally end with adopting exploratory methods to investigate the contextual realities of the employment verification across sectors and to identify which components of the traditional CV can be feasibly substituted with VCs. Exploratory techniques such as stakeholder interviews, process walk-throughs, and industry document analysis were employed to uncover current practices, pain points, and expectations among HR professionals and employers. These insights informed the scope of the system design, shaped key functional requirements, and enabled the formulation of research hypotheses for deductive testing. The exploratory phase thus served as a foundational step in aligning decentralized technologies with real-world recruitment workflows and trust models.

3 EMPLOYMENT PROCESS & VERIFICATION: Contextual and Theoretical Exposition

The evolution of Human Resource Management (HRM) has significantly transformed modern recruitment and selection processes. Scholars such as [165],[164], have extensively documented this shift from traditional personnel management to strategic HRM. Hiring decisions are now based on structured, competency-driven frameworks rather than administrative procedures. This transformation reflects broader changes in workforce dynamics, economic conditions and technological advancements, all of which influence how organizations attract, assess and select talent.

Historically, recruitment has been highly a manual and localized process, relying on word-of-mouth recommendations, classified advertisements, paper-based verification, and in-person interviews. As organizations expanded and labour markets became more competitive, formalized hiring frameworks have emerged, introducing structured job descriptions, competency mapping, and standardized assessment criteria. Overtime, HRM has also evolved to incorporate knowledge management, ensuring that hiring decisions align with both individual potential and organizational needs[141]. Thus, from this body of knowledge, it can be logically deduced that the mechanism enhancing the credibility and efficiency of information conveyed in CVs especially in the verification of qualifications and employment competencies, can significantly improve hiring accuracy and reduce risk in response to the current developing landscape.

A second theoretical implication emerges from the rise of data-driven HR practices. The use of human capital analytics has made it possible to quantify candidate suitability, transforming hiring into a more evidence-based process. This implies a growing demand for structured, trustworthy, and verifiable employment data, needs that are only partially met by the current document-based CVs, reference checks and other accompanying documentation involved. Hence, given modern hiring increasingly dependent on trustworthy and quantifiable data, of which traditional CVs can offer only self-asserted claims, a system enabling the issuance and validation of cryptographically verifiable employment credentials would logically align with the evolving expectations in this domain.

Additionally, as labour markets have become more globalised, recruitment has expanded beyond geographical boundaries, requiring companies to adopt scalable and standardised hiring processes. This shift has increased reliance on digital platforms, job portals, and recruitment management systems, streamlining the process of sourcing, screening, and selecting candidates. However, despite these advancements, traditional hiring practices remain deeply rooted in many industries, often creating inefficiencies, inconsistencies, and challenges in terms of employment verification. Hence, for this study, it follows that integrating SSI and VCs into the hiring process offer a coherent solution to bridge this gap. These technologies promise structured, tamper-proof and machine verifiable proofs of employment informations aligning with the principles of strategic HRM and digital hiring infrastructure.

In light to these theoretical insights and technological imperatives, we now turn to a structured examination of the employment process as a whole. First we unpack the hiring lifecycle, exploring how organizations initiate and manage the search for talent. This is followed by a close examination of the application process and candidate submissions, with emphasis on the flow of information, documentation practices, and existing verification bottlenecks. Subsequently, we investigate industry-specific employment verification requirements, identifying patterns, regulatory expectations, and contextual differences that influence verification rigour across sectors. Finally, we

scrutinize CV as both a communication artifact and a structural container of employment claims considering its limitations, vulnerabilities and opportunities for digital transformation through verifiable credentials. Together, these layers provide a comprehensive foundation for evaluating how decentralized identity systems and VCs can help reform, help improve trust and secure the employment verification process across institutional boundaries.

3.1 THE HIRING PROCESS

The hiring process is a structured series of steps designed to identify, evaluate, and onboard the most suitable candidate for specific role. While the general steps, job definition, sourcing, assessment, selection and verification remain broadly consistent across industries[21], their execution varies depending on organizational context and technological maturity. Thus given the diversity of practices across sectors our research adopts an exploratory approach to understand how employment verification is conducted in different organizational settings. Through qualitative analysis of HR workflows, job documentations, and stakeholder input, we seek to identify the challenges and pain points associated with the verification phase, more so where manual processes document-based evaluations and jurisdictional discrepancies persists[122].

Historically, as stated in section 3, recruitment relied heavily on manual methods, including paper-based CV evaluations, face-to-face interviews and employer references. However, modern recruitment strategies now integrate technology-driven solutions, such as AI-based screening, automated verification systems, digital credentialing platforms. Yet, despite these advancements, employment verification remains a major challenge, particularly in case of credential fraud, lack of standardization, and inefficiencies in verifying qualifications across different jurisdictions. From this observation, and based on the premise that digital trust mechanism can enhance the credibility and auditability of shared information, we deduce that integrating such technologies into the verification phase can improve both accuracy and resource efficiency. This deduction forms the basis for proposing a decentralized system to automate the verification of parts of the CV components.

3.1.1 Identify The Hiring Need and Planning

The hiring process begins with an assessment of organizational needs, ensuring alignment of with strategic business objectives[136]. Workforce planning is essential for evaluating skill gaps, succession planning, and talent management strategies. At this stage decision-Makers outline verification protocols, including the extent of background checks, required documentation, and compliance measures[73].

organizations also determine whether to source talent internally or externally. internal hiring may involve promotions or role transitions, while external hiring requires outreach efforts through job postings, recruitment agencies, or digital hiring platforms. This phase also includes decisions on employment verification methods, such as manual checks, third party verification or digital credentialing solutions[123].

3.1.2 Job Design and Description

At this phase, a well-defined job description is crucial for attracting the right candidates and ensuring transparency in the selection process. Here a job description typically includes;

- Key responsibilities and performance expectations
- Required qualifications (e.g., education , certifications, technical skills)
- Desired competencies (e.g., leadership, problem-solving, team work)

Employers must clearly articulate job requirements to prevent mismatches between expectations and candidate capabilities. A structured job profile also simplifies the verification process, ensuring relevant credentials and qualification can be efficiently validated[82].

3.1.3 Advertisement and Recruitment

Organizations advertise open roles using various platforms such as job boards, company websites, social media and traditional channels like newspaper[106].Active recruitment methods, including reaching out to potential candidates via networks[97], are employed to build a strong talent pool. High-prestige roles often rely on professional referrals and targeted outreach to secure suitable candidates.

Modern practices include company websites, social media, and job boards like LinkedIn for broader visibility Hiring teams also engage in active recruitment by reaching out to potential candidates to secure the best fit for the role [123].

3.1.4 Screening and Verification

While sourcing and selection are front-end processes, screening and verification represent back-end operations primarily handled by employers. This stage, often overlooked in system design, is crucial for establishing the authenticity of the applicant’s claimed qualifications and experience.Activities include;

- **Past Employers outreach:** verifiers directly communicate with previous employers ”Phoning Home” to confirm job roles, tenure, and responsibilities
- **Reference Checks:**Personal or professional references are contacted to assess the candidates’ credibility and character, and in this space, it is been considered a legally constrained area as compliance and regulation tend to play a pivotal role in how much personal information can be shared.
- **Document Validation:**HR teams manually verify certifications, academic credentials and other relevant documents
- **Special Assessments:**Candidates may undergo logical reasoning tests, Korn Ferry assessments, performance evaluations or psychometric assessments, depending on the role.
- **Field investigations:** For roles in law enforcement, detailed background checks, community inquiries and face-to-face interviews may be required.On this note, its emphasized in many cases, candidates are required to make in-person appearances during the process. These appearances allow identity confirmation and ensure authenticity through biometric verification or formal interviews.

Thus, from a critical realist perspective, we recognise that the employment verification is influenced by both technical mechanisms, e.g credential documents and deeper social structures like legal constraints, institutional trust,HR norms. The mere presence of a

credential does not establish trust; what matters is the mechanism of its issuance, the credibility of the issuer, and the ability to verify it securely.

In many sectors e.g healthcare, law enforcement, and finance, verification processes are even more rigorous. For these, the design of any SSI-based system must not only accommodate formal credential issuance but also align with contextual norms such as regulatory requirements, data minimization, and compliance protocols.

3.1.5 On-boarding and Integration

The final stage involves onboarding and integrating new hires into the organisation. A successful onboarding relies heavily on the accuracy and reliability of the verification stage, ensuring new employees are well-prepared and equipped for their roles

3.2 APPLICATION PROCESS AND SUBMISSION

The application stage bridges employer expectations and candidate self-presentation. Applicants curate their submissions, CVs, cover letters, portfolios according to the perceived norms and standards of the industry. This dynamic introduces subjective signalling that recruiters must interpret, and often validate manually. The efficiency and structure during this process directly impact both the quality and diversity of applicants entering the hiring pipeline. Scholars [21], [122] argue that, the application process functions not only as first impression but also as an initial filtering mechanism shaping the likelihood of a candidate advancing through subsequent recruitment stages.

To understand the composition, variability, and verification challenges of application materials exploratory analysis was conducted on CV structures, resume formats, and supporting documents across industries. This revealed which CV elements are typically validated and thus suitable for substitution with verifiable credentials.

Research in industrial organizational psychology has also highlighted that the behaviour of applicants is significantly influenced by the way job opportunities are packaged [27]. Candidates' perceptions of job descriptions, company branding, and application complexity determine their level of engagement and willingness to complete the application process. This reflects the interaction between observable mechanism resume parsing, keywords filtering and the underlying causal structures like applicant inequality, system bias. A realist lens acknowledges that improving verification requires addressing both technical, i.e standardizing credential schemas, and contextual dynamics like job market expectations, digital literacy.

Additionally, applicants often tailor their self-presentation strategies, sometimes exaggerating qualifications or omitting unfavourable details, to align with the expectations set by employers [100]. This psychological dynamics introduces ethical and practical concerns, affecting both employers' hiring decisions and the credibility of the submitted applications. Thus based on established hiring theories, the recurring challenges of unverifiable in resumes, we deduce that credentializing relevant CV components using SSI backed verifiable credential would allow employers to independently verify the claims presented without relying solely on subjective interpretations or follow-up investigations.

To provide a comprehensive understanding in the applicants application process, this section explores the key theoretical and practical components and process of employment application and submission by a job seeker, from document preparation

process to potential barriers encountered when an applicant decides to make an application.

3.2.1 Resume and Application document Requirements

Resume and application documents highlights an important initial requirement component in a job seekers process. This highlight the phase where the job seeker gathers and collect relevant documents required for a role. This application component and requirement plays a significant role in signalling an applicant's qualifications, competencies, and alignment with the job requirements.

According to signalling theory, [32], job seekers strategically craft their resumes or CVs, cover letters, references, motivational letters, portfolios, and supporting documents to present a compelling case for their candidacy. Employers, in turn, interpret these materials as signals of an applicants' potential performance, work ethic and suitability for the role.

Given that, resumes and CVs are often considered the single source of truth in the hiring process. Well well-structured, detailed, and customized application significantly increases the chances of progression through the recruitment pipeline. In contrast, poorly articulated or incomplete submissions may create negative perceptions, potentially disqualifying applicants early in the selection process.

CVs effectiveness is also influenced by ATS in modern day recruitment, where many employers use to screen applications. These systems scan keywords, job-specific qualifications and formatting consistency, making it essential for candidates to tailor their documents accordingly [122].

Due to this, applicants tend to invest more time and resources in the process in order to compete for a job function within an field. Depending with the detail and information captured within a CV helps understand and get a prior assessment of a candidate. Thus looking into each and very document involved preparation process.

- **Resume(CV):**

A CV is a structured document that outlines applicant's truths, these include personal information details, educational background, pre-professional experiences, skills, and achievements. The structure and level of details required vary by industry. For example, In corporate sectors, such as finance, management and IT, resumes emphasize quantifiable achievements by the applicant, leadership, roles, and technical proficiency. In non-corporate fields such as academia, research, and healthcare, detailed educational credentials, publications and certifications hold more weight in determining an applicants suitability. Also, looking into creative industries including design, advertising, fashion, and media, applicants often incorporate visual elements and interactive portfolios alongside traditional CVs to showcase skills.

In 3.4, we look into the CV structure and its component in details providing a fundamental understanding of its importance in the hiring and employment process.

- **Cover letters:**

Though not universally required, cover letter provide applicants with a platform to personalize their application by addressing the hiring manner directly, emphasizing key achievements, and articulating how their skills align with the specific role or organization. Studies indicate that tailored, role specific cover letters can enhance applicant credibility and increase likelihood of being shortlisted for interview [21]. However, in the current form, cover letter are inherently self-asserted

narratives, lacking any embedded or referenced verifiable information. The identity and qualifications of the author are typically inferred only from the name and contact details provided, without any proof or linkage to verified credentials. As such, while they serve as persuasive tools, they remain vulnerable to embellishment, misrepresentative, or impersonation underscoring the need for enhanced mechanisms of trust and verification in the applicant communication process

- **Portfolios and Supporting Documents:**

In various professional domains, portfolios and supporting documents serve as essential complements to the CV, offering tangible evidence of an applicant's skills and qualifications. For example, graphic designers, architects, and software developers commonly submit visual or interactive portfolios to showcase their technical and creative capabilities. In academia, healthcare, and engineering, applicants may include research publications, clinical case studies, patents, or technical reports as supporting documentation.

In regulated industries such as law, finance, and healthcare candidates are often required to present formal certifications, licenses, or compliance documentation as proof of eligibility and professional standing. These documents are typically verified through visual trust indicators including official logos, institutional letterheads, handwritten or digital signatures, wet-inks seals, stamps, and explicit naming of the issuing authority. While these markers serve as conventional methods of establishing document authenticity, they are still susceptible to forgery and require manual inspection posing limitations in terms of scalability, efficiency and security in modern digital recruitment.

- **Motivational letters & References:**

In sectors as such education, NGOs, and international organizations, motivational letters are commonly required. These letters allow candidates to articulate their values, career aspirations and commitments to the organization's mission. References on the other hand either professional or academic further validate an applicant's credibility, providing insights into their past performance and professional conduct [27].

Just like Cover letters, both motivational letters and reference letters are largely narrative-based and self-asserted, lacking embedded mechanisms for objective verification. The credibility of references typically relies on indirect trust makers such as named referees, institutional affiliation, job titles, signatures and contact information, which are manually reviewed by hiring teams. A good example of a provided reference letter is depicted in A5. While these traditional methods offer some level of assurance, they remain vulnerable to fabrication or exaggeration and often require time-consuming follow up by the employer highlighting the need for more structured, verifiable and tamper-resistant approaches in validating character endorsements and personal motivations

- **Identification & legal Documents:**

In cross-boarder employment scenarios, the submission and verification of personal identification documents are essential, though requirements vary depending on industry norms, regulatory obligations, and organizational policies. While many employers typically request identification documents such as national ID cards, Passports, or residence permits after the interview stage, certain sectors,

particularly government agencies, security-sensitive industries, and financial institutions often mandate early identity verification in accordance with Know Your Customer (KYC) regulations and risk management protocols.

The current verification process largely relies on manual inspection of physical and visual elements embedded in the documents, including photographs, holographic seals, machine-readable Zones, watermarks, barcodes, and official stamps, as well as the issuing authority's name and logo. These features are designed to deter forgery and enables first-line validation, often with the aid of scanning tools or human scrutiny. However, this method is still prone to error, inconsistencies, and regional variations in document standards limiting its effectiveness in remote or large-scale digital hiring contexts. These limitations highlight the growing relevance of digital identity technologies that offer automated, tamper-evident and cryptographically verifiable identification process, particularly in high-trust employment environments.

- **Recommendation Letter & Employment verification**

They provide third-party validation of a candidate's skills and experience. Recommendation letters from employers or professors highlight competencies and character, while employment verification letter confirms job title, tenure, salary, and responsibilities.

- **Education and Professional certifications:**

Educational qualifications and professional certifications remain critical components of candidate validation, particularly for entry-level positions and roles requiring industry-specific expertise. Applicants are often required to submit academic transcripts, diplomas, or degree certifications as evidence of formal education, while professional certifications such as AWS for cloud computing or PMP for project management as classic example in the Figure A6, serve to demonstrate specialized skills and up to date domain knowledge.

Verification of these credentials typically depends on visual trust markers including institutional logos, official letterheads, authorized signatures, embossed seals and certificate serial numbers. In some cases, employers may also contact issuing institutions directly or rely on third-party background check services to confirm authenticity. However the methods are often time-consuming, manually intensive and vulnerable to document forgery or misrepresentation.

- **Compliance and Background Check Document**

These are essential component in the application process for verifying a candidate's background, ensuring workplace security, and meeting industry regulations. For instances, background check authorization is commonly required in financial institutions like banks to access criminal or financial history.

Beyond document quality, applicant motivation also influences submission behaviours. Expectancy theory [175] suggests that candidates are more likely to invest efforts in application preparation when they perceive a high likelihood of success. This means that clear job descriptions, transparent hiring criteria, and well-defined career progression pathways positively impact an applicant's engagement level. Conversely, complex or ambiguous application processes may discourage potential candidates from completing their submissions [167].

3.2.2 Application Documents Preparation Process

Job seekers must tailor their application materials to meet employer-specific requirements. The integration of technology into recruitment has significantly transformed this process, shifting from traditional paper-based, handwritten CVs and printed document submissions to full digital platforms. Today, employers utilize various application tools and platforms, such as ATS, AI-driven resume screening and online job portals, to streamline hiring, enhance efficiency and access a broader talent pool[130],[95].

These advancements have optimized recruitment workflows, however, they have also introduced challenges for applicants. Job seekers must navigate multiple systems, adapt to different submission formats and comply with varying platform-specific requirements to ensure their applications are received and processed correctly[12]. Research indicates that ATS often filters applications based on keyword matching and formatting criteria, potentially disadvantaging candidates who fail to optimize their resumes accordingly[171]

Theoretical and empirical studies provide valuable insights into how these digital tools influence hiring outcomes, applicant behavior, and the overall effectiveness of recruitment process. Digital recruitment systems have been shown to improve hiring speed and efficiency, however, concerns remain regarding biases in AI-driven screening tools and the lack of standardization across platforms [150],[10]. Candidates' employability is not solely determined by their qualifications but also by how effectively they navigate these digital platforms and adhere to the diverse expectations of employers[28].

1. Document creation and preparation tools

Before submitting applications, applicants must prepare their documents in line with employer expectations, as outlined in 3.2.1. To enhance their visibility, job seekers rely on various document creation and editing tools, each providing unique advantages and limitations. Research by[18], provides insights into how these tools shape communication in hiring, affecting readability, accessibility and compatibility of resumes and other application materials. Different document formats vary significantly in their ability to structure and convey information effectively. Rigid formats such as PDF and LaTeX provide higher clarity and maintain document integrity, but offer less flexibility for quick modification. In construct, open formats like Microsoft Word and Google Docs facilitate easy modification but may introduce inconsistencies in layout or structure when parsed by ATS [10].

The landscape of document creation has evolved, with numerous digital tools catering to various industry needs. Microsoft Word is the most commonly used resume creation tool due to its broad acceptance by employers and compatibility with ATS, ensuring seamless keyword parsing [178]. Adobe PDF, while ensuring document integrity, may present parsing issues in ATS if not optimized. LaTeX is favoured in academic and scientific sectors for resumes that require a structured section. The Europass CV Builder promotes standardization across EU member states, aligning with regulated hiring frameworks[12].

Job seekers often adjust the complexity and visual appeal of their resumes based on the industry-specific expectations. For instance, creative roles may benefit from visually enhanced designs, while highly structured, text-based resumes are preferred for technical or executive positions, where ATS parsing is a priority. This strategic

approach helps applicants maximize their chances of securing interviews in their target industries

2. Application Documents submission

Just like in the document creation, the transformation has been significant. Modern hiring practices now rely on a variety of digital platforms, each with unique interfaces, submission requirements and advantages. We highlight the principal types of application platforms, with their functionalities and implications on both the applicants and employers.

- **Job boards and Professional Networks**

Job boards and professional networks serve as primary channels for mass recruitment. These platforms allow employers to reach a broad audience and enable candidates to apply directly online. For instance, LinkedIn functions as both a professional networking site and a recruitment platform, enabling direct applications and active recruiter engagement [117].

Indeed, Glassdoor and Monster are general job boards that offer extensive posting capabilities with integrated application features, thereby increasing visibility and streamlining candidate tracking.

- **Company Career Portals**

Many organizations now prefer candidates to apply directly through their own career portals. These platforms typically require applicants to create user profile, manually enter professional details and upload supporting documents. Although direct submission fosters closer employer-candidate engagement, they often require repeated data entry, which can be time consuming and may lead to errors

- **Email-Based Applications**

Despite the rise in specialized platforms, email application remains prevalent, particularly in SMEs and in sectors where traditional practices persist. Applicants attach their documents via standard email services.

Some Recruitment agencies and headhunters also play a pivotal role in matching candidates with suitable positions, particularly for specialized or executive roles. These intermediaries can enhance applicant visibility by presenting resumes to multiple employers, however they may also impose fees or require exclusivity agreements

3.3 INDUSTRY SPECIFIC EMPLOYMENT REQUIREMENTS

The evolution of employment verification is not monolithic, rather, it is shaped by sector-specific regulatory frameworks, operational risks, and credentialing norms. Industries such as healthcare, finance, defence, and academia impose distinct verification requirements based on the sensitivity of the role, regulatory obligations, and the nature of professional competencies. These sectors illustrate the structural variability in verification practices and underscore the need for context-sensitive trust mechanisms.

In this exploration we apply a critical realist lens to understand how observable verification practices in each sector are shaped by the underlying institutional mechanisms, such as risk tolerance, compliance culture, and labour regulations. For example, while background checks are visible procedural steps, they are underpinned by assumptions about trust, risk mitigation, and accountability that vary by

industry. These real structures shape the surface-level diversity in how employment credentials are treated, verified, and trusted. Furthermore, it forms part of the problem awareness and requirement elicitation phase in the design science methodology. Understanding how employment verification functions across different domains is critical to designing a solution that is technically valid, socially acceptable, and institutionally compliant. The knowledge gained here directly informs the artifact's functional and non-functional requirements.

3.3.1 Health care and Finance

In these highly regulated sectors, employment verification processes are key to ensuring operational integrity, compliance with legal standards, and the protection of human, financial assets. Enhance verifying the credentials, certifications and professional histories of employees in these sectors are not merely a human resource function, rather it is a critical risk management practice with direct implication for public safety and institutional trust[30]. Research has consistently demonstrated that failures in employment verification in these sectors can result in severe consequences, including malpractices, financial fraud, regulatory penalties, and reputational harm[143].

In healthcare sectors, employment verification is indispensable to ensure that professionals such as doctors, nurses and pharmacists are entrusted with responsibilities that have immediate and profound impacts on patients' well-being. Some of the essential components of the healthcare employment personnel verification includes;

- **Professional licenses and Certifications:** Practitioners must possess valid licenses issued by accredited regulatory authorities. These licenses, such as those for registered Nurses or Medical Doctors often require periodic renewal tied to continued professional development and compliance with updated medical standards[57].
- **Educational background verification:** Accreditation of medical and nursing education institutions is crucial to ensure that the practitioner have received appropriate clinical training and theoretical knowledge[70].
- **Clinical Employment History:** Reviewing prior employment records verifies the scope and quality of clinical experience and reveals any patterns of pre-professional misconduct, malpractice claims or disciplinary actions[33].
- **Background Screening:** Criminal history and malpractice checks help healthcare organizations mitigate legal risks and uphold patient trust.

Ideally, the current credentialing process in these sectors are typically with one central authority, they also include manual processes during acquisition and verification, and they are majorly fragmented across multiple jurisdictions making them prone to significant delays when required. Errors in the credential verification have been linked to catastrophic patient outcomes and legal liabilities under the doctrines of corporate negligence and vicarious liability[30]. Given the dynamic nature of the modern day healthcare, including the rise of telemedicine and international workforce mobility, traditional models are proving to be increasingly insufficient.

Thus, decentralized verification models based on SSI principles offer a transformative alternative as they hand over power back to the users and optimizing the trust levels between the employers and employees within these sectors without fear of the consequences. Since, by utilizing Verifiable credentials, healthcare institutions can

achieve real-time, cross-boarder verification of professional qualifications, history and competencies, thereby, enhancing operational efficiency while maintaining data integrity and patient safety[54].

On the other hand, in Finance industry, the employment verification processes is integral for protection against internal fraud, ensuring regulatory compliance and maintain fiduciary responsibility. Financial institutions must ensure that employees handling sensitive operations or customer assets possess verified competencies and ethical integrity. Just like in healthcare, educational and professional background checks and employment history validation are of utmost importance. Along these key requirements, these elements are also included as requirements within this sector;

- **Regulatory Compliance Verification:** Screening through databases maintained by bodies such as Financial Industry Regulatory Authority (FINRA) in America or The European Securities and Market Authorities (ESMA) identifies any prior disciplinary actions, sanctions, or compliance breaches.
- **AML and KYC Training Verification:** Employees must be certified in Anti-Money laundering and know your customer protocols to prevent financial crimes[76].
- **Financial and Criminal Background:** Institutions conduct checks to assess vulnerabilities to fraud, bribery, or insider threats, especially for positions involving fiduciary oversights [126].

Despite the nature of these process, just like in healthcare sector, verification remains largely manual and fragmented too as they rely on third-party background screening services, thus opening gaps for malicious actors. However, the financial sector embracing Regtech innovations[84], has particularly well-positioned it to benefit from decentralized employment verification frameworks. Enhance, integrating and utilizing VCs with the existing innovations, financial institutions can securely verify a individuals qualifications, regulatory standing, and employment history without relying on intermediaries, thereby enhancing trust, reducing onboarding times and strengthening, compliance audits[1].

Drawing from well-established risk management and compliance theories, our research here deduces that credential verification in these sectors must be, tamper-proof to prevent falsification, should be cross-jurisdictional to support global workflow mobility, and should also be time-sensitive to meet onboarding deadlines and regulatory reporting windows. Based on these premises, we deduce that VC implemented via SSI frameworks offer a logical and technically sound solution for these sector. Their cryptographic assurance, interoperability, and revocation support align with the industry's needs for fast, verifiable and compliant credential handling, hence, contributing directly to the design objectives of the system artifact, particularly in defining the schemas for VCs, Issuer registry integration and revocation.

3.3.2 Police and Military Recruitment

In Industries and profession like police and military recruitment, the verification process over decades have been even more rigorous, reflecting the sensitive nature of roles and their impact on national security and public safety. Unlike many civilian jobs, these positions demand a higher level of scrutiny due to candidates' access to classified information, weapons, and public authority. The verification process typically involves;

- **Background Checks:** Detailed criminal record investigations to ensure candidates have no history of illegal activities

- **Identity Verification:** Confirmation of personal details, including biometrics, to establish the authenticity of who they claim to be
- **Educational and Training Credentials:** verification of academic qualification and any prior training certifications relevant to the positions
- **Psychological and Medical Assessments:** Screening for physical fitness and psychological stability to ensure candidates can meet the demands of the job
- **Reference checks and Field Investigations:** interview with previous employers, academic institutions, and personal references, often supplemented by direct investigations within the candidates' local community or environment
- **National Security vetting:** For roles in the military additional steps like security clearance checks are undertaken to assess candidates' loyalty and potential vulnerability to espionage or corruption. as this applies to organizations such as TERMA [109]

While these verification steps are observable, they are grounded in deep national security structures, patriotism based trust models, and state-controlled risk assessments. A realist stance highlights that verification here is both a technical and political act, shaped by the sovereignty, loyalty, and institutional doctrines. Given the requirement of non-repudiation, data integrity, and biometric assurance, it is also deduced that decentralized identity systems using DLT with selective disclosure and DID-authentication mechanism can improve verification precision while reducing the administrative delays.

3.3.3 Academia

In academia, the focus shifts to verifying the authenticity of degrees, publications, and research affiliations, which are critical for ensuring institutional credibility and compliance. Verification processes must confirm the legitimacy of academic accomplishments and safeguard against issues like degree fraud, plagiarism, or falsified research credentials. This is especially important when institutions hire international candidates, where credential validation becomes even more complex due to variations in educational systems. Thus the challenge lies in global variations in academic systems, manual transcript exchanges, and lack of credential interoperability. Literature reviews and case comparisons of academic hiring practices across countries were used to map out inconsistencies in credential validation. For example, non-standard degree titles, missing digital records, or unverifiable foreign institutions were identified as recurring barriers.

According to Signalling Theory, job applicants and employers often have conflicting interests, with applicants seeking high-salary positions and employers aiming to recruit skilled candidates [15]. This dynamic creates a risk of inaccurate information sharing, leading to hiring decisions based on falsehoods, which can have catastrophic consequences for organizations. Thus we deduce that issuing academic VCs tied to university-verified DIDs, credential schemas like EDCI-compliant and ORCID-linked research IDs offer a trustable and scalable alternative.

Despite the critical nature of these processes, traditional verification methods across these domains share a common challenges. Over reliance on centralized systems, manual data retrieval and third-party intermediaries often results in inefficiencies, high cost, and increased risks of data breaches. Moreover, existing systems frequently lack transparency,

making it difficult for all stakeholders to fully trust the process. As [69] puts it, transparency raises tensions as on one hand it facilitates employee empowerment and on the other hand it drives employee surveillance and privacy concerns.

The emerging of Web3 economy and the Blockchain's massive adoption in 2021 with technologies such as SSI and DLT offers innovative solutions to these challenges. SSI enables individuals to own and control their credentials, ensuring privacy while simplifying the verification process. Meanwhile DLT provides immutable, transparent records that enhance trust and eliminate tampering. For industries such as police and military, these technologies can streamline background checks and security clearances ensuring real-time, tamper-proof validation of credentials and reducing administrative burdens. where as in civilian jobs the historic labour-intensive, time-consuming and costly process like "Phoning Home", letters and direct communication with different stakeholders as mentioned in A.3.2 above compelling organizations to outsource services with external providers such as workday, Taleo as part of the verification process much easier and simpler.

3.3.4 Remote Works

The widespread shift towards remote works has significantly altered the hiring practices since 2021 post-COVID, emphasizing on digital methods that often lack sufficient rigour. Typically, remote recruitment process involve document-based identity verification, such as requesting scans of passports, national IDs, conducting asynchronous or live video interviews and reliance on third-party background checks or the reputational metrics of online platforms[115]. However, these approaches remain highly fragmented, vulnerable to manipulation and lack standardizations.

Emerging evidence underscores the scale of this vulnerability. Candidates have exploited VPNs, synthetic identities, and forged documents to bypass conventional screening protocols. Notably, investigations have revealed cases where North Korean IT operatives successfully infiltrated international organizations by posing as foreign citizens using fabricated professional profiles and falsified identity credentials[94]. These deceptive practices have not only allowed sanctioned actors to evade international restrictions but also have exposed employers to severe legal, reputational and compliance risks[177].

Furthermore, documented cases of video interview manipulation as stated 1.1, including the use of deepfakes, voice spoofing, and paid proxies have revealed that individuals appearing in a virtual interview may not be the person who ultimately accepts and perform the job. Such incidents exacerbate the risk of insider threats, ranging from intellectual property theft to system compromise through malware insertions or unauthorized access[132],[39]. These findings point to systematic weakness in the current digital infrastructures, especially in high-risk or sensitive industries.

In conclusion, the global shift to remote work has exposed fundamental flaws in identity verification, particularly in verifying who a person is, what they've done, and where they've worked as shown with the case of deepfakes, proxies, and fake profiles above illustrating trust breakdowns in the digital hiring environment. It introduces observable verification mechanisms, video calls, ID scans but lack real trust anchors. A critical realist interpretation sees the problem not just a UI/UX issue but as a breakdown of casual trust structures, we assume that what we see digitally corresponds to reality but it may not. Additionally, synthesis of recent investigative reports used to document trust failure points, helps refine risk mitigation strategies embedded in the artifact design[42]. It is deduced that remote verification must; minimize exposure of

personal data, prove source authenticity of credentials, and support zero-knowledge or selective disclosure proofs.

3.4 CV STRUCTURE AND ITS COMPONENTS

A CV serves as a structured narrative of applicant's professional and academic history, presenting self-asserted claims regarding personal identity, educational background, work experiences, skills and achievements. While the CV functions as a primary source of truth in the hiring process, it is ultimately a high-level summary one that requires supplementary documentations highlighted in 3.2.1 to verify the accuracy and authenticity of the information it contains.

The structure, content, and emphasis of a CV often vary across the above named industries in 3.3. In corporate sectors they tend to highlight quantifiable accomplishments, leadership roles, and technical proficiencies. In contrast, fields like academia, research, healthcare place greater importance on educational qualifications, peer-reviewed publications, and formal certifications. Meanwhile, applicants in creative industry frequently augment their CVs with portfolios and visual that demonstrate artistic and practical competencies.

However, regardless of industry, the claims made with a CV typically require additional proof in the form of original documents such as diplomas, transcripts, employment contracts, or reference letters. This dependence on external documentation underscores the need for verifiable representations of these credentials, particularly in digital hiring environments where manual validation is impractical or prone to error.

Thus in this section we delve deeper into the structure and components of the CV itself, outlining its significance in the employment process while highlighting the limitations that motivate the integration of cryptographically verifiable credentials to enhance data credibility and streamline verification. Moreover it draws on exploratory methods, including document analysis and review of HR best practices in our discussions, to map the standard structure and functional role of CV components. This enables the identification of which sections are most commonly reviewed and subjected to verification processes. Exploratory insights have also revealed industry-specific variations in emphasis and structure, such as quantitative performance in business roles versus publication records in academia. Figure 2 illustrates the structured CV which includes the following elements:

Personal information and contact Details

This section provides essential identification and communication details, including; Full name, Professional Title (optional), Phone Number, Email address, LinkedIn Profile (if applicable) and Personal websites or portfolio. Employers rely on this information to verify candidate identity and establish initial contact. Some jurisdictions have legal restrictions on including certain Personal details, Such as age or marital status to prevent discriminatory hiring practices.

Professional Summary or Personal Statement

A professional summary offers a concise overview of candidate's expertise, career aspirations and unique value proposition. This section is particularly useful for senior professionals and those transitioning between industries as it helps recruiters quickly assess alignment with job roles. This is commonly used for quick screening by HR professionals.

Work Experience This is considered one of the most critical parts of the CV as it

outlines a candidate's career history, job responsibilities, and key achievements. Best practices suggest structuring this section in reverse chronological order, ensuring recent and relevant roles are emphasized. Each entry typically includes ; Job Title, Company Name and Location, Employment period (start and end dates), Key responsibilities and achievements. Studies also suggest that quantifiable achievements like increased sales revenue by 30% or Led a team of 10 engineers significantly enhance CV effectiveness in Competitive job markets. This section is often the focus of manual verification via references or prior employer contact.

Educational background:

This provides details on academic qualification , which are particularly relevant in industries requiring specific degrees or certification. Each entry includes the degree name, institution and location, year of graduation and key achievement or work course if relevant.

Skills and competencies

Employers often use skills-based hiring approaches, where a candidate's technical and soft skills play a central role in recruitment decisions. The elements include; technical skills like programming languages, software proficiency and data analysis for IT job seekers or professionals, soft skills, such as leadership, communication, teamwork and certifications and professional training.

certifications

and professional membership this highlights the industry-specific recognized credentials that demonstrates candidate's commitment to continuous professional development.

References while some employers request references upfront, others prefer to request them later in the hiring process and this typically includes name of their referee, their professional titles or just contact detail. Frequently used in trust-sensitive sectors.

Base on the logic of verifiability and the premise that hiring processes value third-party-authenticated information, we deduce the CV components such as educational qualifications, employment history, certifications, and professional memberships are most suitable for credential substitution using VCs. This deductive insight informs the architecture of the SSI-based system development in this project by contributing to the design requirement specification by identifying what data types the system must support. Which components may require selective disclosure capabilities, and which issuers can be integrated into the ecosystem.

PERSONAL INFORMATION & CONTACT

JOHN DOE

+123-456-7690 | email@example.com
City, State | linkedin.com/in/johndoe

PROFESSIONAL SUMMARY OR PERSONAL STATEMENT

Results-driven professional with over 8 years of experience in project management and team leadership. Skilled in managing multiple projects simultaneously, optimizes processes, and delivering results on time and within budget. Strong communicator with a proven track record of building and leading high-performing teams.

WORK EXPERIENCE

Project Manager • Company ABC | Mar 2019 - Present
City, State • Present

- Successfully managed multiple projects across-arulobly, through effective aon:
- Conducted client and stakeholder communicate in mannent project tasks,
- Improved processes, resulting in a 16% increase in efficiency in efficiency.

Assistant Project Manager • Company XYZ | Jun 2015 - Feb. 20119
City, State • February 2019

- Supported project managers including project managers, with precision, an:
- Assisted in budget tracking, as well as coordinating project activities, and cond:
- Coordinated project activities in project coordination tasks.

EDUCATION

Master of Business Administration
University of YYZ

Bachelor of Science in Business Administration
University of ABC

PORTFOLIO

Portfolio project description or link

CERTIFICATIONS

Project Management Professional (PMP)

SKILLS

- Project Management
- Team Leadership
- Process Improvement
- Budgeting & Forecasting
- Agile & Scrum
- Client Relations

INTERESTS

Hiking, Travel, Photography

REFERENCES

Available upon request

Figure 2: An Example of a CV and its Component

3.5 Barriers and Challenges in the Process

The hiring process has increasingly been complicated by various barriers and challenges for sure, particularly, in ensuring compliance with data privacy regulations such as GDPR, NIST Cyber security Framework, eIDAS 2.0 and AI Act, crucial but however, remains challenging for organizations to maintain during the recruitment processes. Those compliance regulations majorly impact how employers collect, store, and process applicants' data and information.

In addition to compliance, the application preparation and submission process for job seekers furthers challenges. Where Job seekers often faces difficulties meeting specific employers requirement for CV customizations and adhering to platform-specific guidelines resulting in time-consuming processes, where applicants must tailor their CVs and other documents to every job application to formats described in process 3.2.2 above, ensuring they meet the unique demands of each role, which can lead to missed deadlines, rejection due to formatting issues, or failure to comply with specific application instructions. Applicants also bear the cost of recruitment platforms and associated fees, often exacerbating the financial burden, especially when multiple applications are being made.

Further into the challenges lies increasing reliance on AI-driven recruitment tools further complicates the process, as candidates must optimize their applications for ATS to ensure they are not filtered out. In addition to this, the recruitment process itself requires candidates to navigate various industry-specific requirements. For example, technical roles may require a portfolio of work done or specific constrictions, while creative roles may emphasize aesthetic presentation in CVs. These requirements not only adds an extra layer of complexity, but also making it difficult for job seekers to adapt quickly and effectively.

The verification process of applicants' credentials also brings another dimension to the challenges, as employer must ensure the accuracy of submitted information and verification against time constraints and financial costs becomes a critical issue, especially when a company must verify the qualifications of multiple applicants, often leading to delays and inefficiencies due to the resource required. Thus current practices in job applications like face to face interviews, and networking reflects in this outdated practices such as the inclusion of home addresses in CVs, despite the growing emphasis on remote work and privacy concerns.

Unverifiable documents complicates the current process as large number of job seeker submit CVs with unverifiable information, whether due to inaccuracies, incomplete data or even intentional falsification as research has shown that 81% of applicants fail to quantify their achievements in their CVs, while 80% use AI tools to tailor resumes [26]. While networking remains an essential part of the job search, especially on platforms like LinkedIn, where data shows a 27% increase in response rates when mentioning a mutual employer in communications, these efforts still face limitations in proving the authenticity of claims made on resumes [116]. With this assumptions that Unverified CV claims erode hiring accuracy and increased risk, we deduce that aggregating these claims into a digitally verifiable, issue-signed credential format can enhance trust, reduce employer efforts, and streamline candidate verification.

4 TRUST IN EMPLOYMENT VERIFICATION;The Evolution from Traditional to Digital Paradigms

Trust is a concept deeply embedded in both human interactions and digital ecosystems, recognized as a multifaceted idea with a variety of operationalizations [145]. In digital environments, trust has frameworks that serve as structured guidelines and emphasis for systems to establish the basis for trusted relationships between various entities in a given network. These frameworks, define how trust is established, validated, and maintained, and they incorporate legal, technical, and behavioural aspects to ensure that all parties involved can rely on the system [125], [184]. Theoretical models of trust, particularly in Human Computer Interaction (HCI), have evolved to accommodate the unique dynamics of this online digital environments, where traditional methods of trust-building are no longer feasible [135].

However, despite the advancements in digital trust frameworks, significant challenges remain primarily due to the limitations outlined in our previous chapter 1.2,3 across different industries and jurisdictions that may lead to inefficiencies in verification processes. Thus heightened risk for job seekers including data breaches and privacy violations and a limited degree of control over their employment records [77], [104] and more particularly pronounced in cross-boarder hiring scenarios where complex regulatory landscapes such as GDPR, electronic Identification, Authentication and Trust Services (eIDAS), plays a role that may inhibit employment mobility [9].

One emerging trend in employment trust models is the integration of digital identity systems and social-linked verification methods where platforms like LinkedIn, Behance, and GitHub function as informal indicators of professional credibility allowing recruiters to validate candidates through peer endorsements and public contributions [128]. But however much these platforms enhance transparency and visibility, they lack formal verification mechanisms, raising concerns about misrepresentation, unverifiable claims and biases in recruitment decisions [180].

And this highlights the fact that traditional employment verification systems have remained largely paper-based and fraught with inefficiencies. Employers often encounter delays, document forgery, and credentials discrepancies, resulting in longer hiring timelines and diminished trust in the hiring process [104]. The absence of Self sovereign initiatives forces candidates to repeatedly submit multiple versions of their CVs and credentials for each job application, increasing administrative burden and redundancies [180].

As HCI research has shown, the role of trust in digital online environments has become crucial, as users interact with systems that would replace face-to-face with more direct and verifiable forms of communication [184]. This paradigm shift necessitates the development of technologies supporting secure, trustworthy interactions in an environment where participants may not share previous relationships or a physical presence making the operationalization of trust defacto for the success of online services [90].

Theoretical foundations in trust theory highlight that trust is often based on reputation, risk, and certainty. Elements adapted for digital interactions where systems mediate trust through personal relationships [81], these concepts are also adapted where;

- **Reputation:** Typically built on prior interactions and can be validated through cryptographic methods and blockchain technologies underpinning systems like SSI [181].
- **Risk** Refers to the potential for fraud, identity theft, or unauthorized access, all of

which are mitigated by robust validation processes within the trust framework.

- **Certainty** Crucial, as entities need confidence that the data they are interacting with is both accurate and unaltered, which is achieved through secure protocols and consensus mechanisms[9].

Historically, trust frameworks have evolved alongside the digital transformation. Early models were more centralized, relying on Public key infrastructure (PKI)[120] and Certificate Authorities (CAs) to validate digital identities. These frameworks were built on the premise that a trusted third party could verify and mediate trust in digital transactions. However, with the advent of decentralized technologies, a new paradigm emerged, wherein trust could be established without the need for a central authority.

The rise of federated identity systems and DIDs represents another evolution in trust frameworks. These systems allow users to authenticate across multiple platforms without needing to create separate identities for each service. Trust frameworks ensure that these identities are secure, interoperable, and compliant with privacy and regulatory standards, such as the GDPR in Europe or KYC [105] regulations in finance.

In SSI, trust frameworks are designed to ensure that when an individual or entity claims an identity, that claim can be verified by external parties without revealing unnecessary personal data. This exchange of claims is essential in allowing decentralized systems to function. The framework ensures that entities can trust each other without relying on a central authority to verify the data. This approach also helps resolve challenges such as privacy and data security, as only the necessary information is shared between the parties involved, rather than exposing sensitive data to potentially vulnerable central systems.

4.1 Importance Of Trust In Employment Verification

At the core of employment verification lies trust. Employers need assurance that the credentials presented by candidates are legitimate, accurate, and tamper-evident[107]. Conversely, candidates seek confidence that their personal data is secure and shared only when necessary and with the rightful party.

Traditional employment verification processes have struggled to establish trust due to several limitations such as them relying on centralized repositories, manual attestations and third-party intermediaries. Each of which introduces potential vulnerabilities. For instance, centralized databases are susceptible to breaches and unauthorized access, and intermediaries may not be transparent or accountable to the data subjects and the lack of candidate's agency over how and when their data is shared raises legitimate privacy and ethical concerns proving how important having trust in systems is important.

Looking further into cross-border hiring scenarios, another layer of complexity is added by the variations in regulatory frameworks that may introduce friction and delay. For instance, verifications in current processes has often involved outdated methods like phone calls, email correspondence and document checks that are time-consuming, prone to error, and inconsistent in reliability as they information source and data authenticity are unverifiable. These inefficiencies can not only slow down hiring processes but also erode organizational responsiveness and competitiveness in the digital-first talent market.

Modern digital technologies offer a paradigm shift in this trust deficiencies by restoring information control back to the user. SSI technologies for example,[154] empowers individuals with ownership and control over their credentials, allowing them to selectively disclose information in a privacy-preserving manner[47]. When coupled

with DLT,[20] verification becomes temper-resistant and auditable, with no need for centralized authorities. These technologies reduce dependency on third-party attestations, mitigate risk of forgery, and enable seamless interoperability across jurisdictions.

As highlighted in section 4, trust in digital verification systems extends beyond the correctness of data, it encompasses confidence in the process of verification itself [71]. Effective identity proofing, as part of this process underpins regulatory compliance and reduces exposure to fraud[51]. By embedding cryptographic guarantees and decentralized consensus mechanisms into identity workflows, SSI and DLT systems provide a scalable, secure alternative to legacy models.

Thus, building trust through digital verification frameworks is not merely a technological enhancement but a strategic imperative. It aligns with broader shifts in digital governance, user autonomy, and cross-boarder employability. In transitioning from document-based to trust-centric verification models, organizations gain improved transparency, integrity, and efficiency in their hiring process, ultimately fostering a more agile and trustworthy labor market[124].

4.2 Identity Proofing in Employment Verification

Identity can be conceptualized in various ways, but for the purpose of our study, digital identity is best understood as the aggregation of all digitized information associated with a natural person, legal entity, or contextual subject of reference. This definition includes both core identity attributes, such as name, data of birth, and address, and context-specific data drawn from different aspects of a subject’s life, including education, employment history, health records, financial details and social affiliations.

In the context of employment verification, identity proofing plays a key role in establishing digital trust. As defined by National Institute of Standards and Technology (NIST) Special Publication 800-63A, identity proofing is the process of collecting, validating and verifying information about a person for the purpose of establishing a valid and reliable identity within a given context[160]. This process is foundational to ensuring that digital credentials are issued to authentic and uniquely identifiable individuals.

To address varying levels of risk, NIST further delineates identity proofing into three progressive levels of assurance, IAL1, IAL2, and IAL3. These levels define the rigour required in verifying identity information, ranging from self-asserted attributes to verified physical and biometric validation, depending on the sensitivity and security requirements of the context;

- **IAL1:** No identity proofing is required.
- **IAL2:** Requires identity evidence to be validated and verified, typically through government-issued documents and corroborating records. In traditional employment verification, most process such as passports, academic transcripts, or employer-issued letters.
- **IAL3:** Demands in-person proofing and physical presence, often with supervised remote sessions and biometric validation

By categorizing identity assurance into discrete levels as above, employers within the employment verification domain can tailor their verification process according to the sensitivity of the job role, jurisdictional requirements, and associated risk profile. For

instance, sensitive role in finance or government may require IAL3-level proofing, while freelance or temporary roles might suffice with IAL2 mechanisms.

In modern digital systems, particularly those on SSI and DLT, identity proofing becomes an integral part of credential issuance. Trusted authorities such as educational institutions or former employers can conduct identity proofing in compliance with NIST guidelines and issue verifiable credentials that are cryptographically signed and bound to the subject's decentralized identifier[25]. This ensures that the credentials presented during the employment verification are both authentic and traceable to an adequately proofed identity.

Moreover, the binding between a verified identity and the corresponding digital representation aligns with the NIST's emphasis on strong identity-to-subject binding, which is essential for maintaining integrity throughout the employment life cycle. Verification platforms can then validate these bindings without string personal data centrally, preserving privacy while ensuring trust.

Digital systems operating in federated or decentralized environments, where trust must be maintained across organizational or national boundaries[74] have two additional assurance levels defined by NIST namely;

- **AAL:** Authenticator Assurance level, where the authentication is strength used when a previously proofed user logs into a system to share or access employment credentials. AAL ensures that only the legitimate identity holder can authenticate and present verified credentials , safeguarding against unauthorized access.
- **FAL:** federation Assurance Level, governs how assertions about identity and attributes are securely conveyed between systems in federated model. For example in a scenario where a university acts as a credential issuer and a multinational employer iis the verifier , FAL ensures that the assertion protocol e.g., OpenID connect or SAML used to transmit identity and credential information maintains integrity, confidentiality and non-repudiation .

Together IAL, AAL, and FAL form a comprehensive trust architecture that supports not only just identity proofing but also ongoing secure authentication, cross-domain verification and federated trust delegation all essential in modern day verification, especially in cross-border hiring, digital on-boarding and SSI-based employment ecosystems [50].

4.3 Trust Models in Employment Verification

A trust model can be defined as a structured conceptual or computational framework that governs how trust is established, evaluated, maintained and revoked between interacting entities such as individuals, organizations, or systems within a specific context[112]. This construct is especially crucial in digital, decentralized, or distributed systems, where the absence of pre-existing relationships necessitates the mediation of trust through cryptographic protocols, digital credentials, and governance frameworks [56].

In the employment verification domain, trust models underpin the assurance that a digital credential such as proof of employment or qualifications can be reliably accepted as valid and authentic by third-party verifiers[14]. These models ensure that trust is not only placed in the credential itself but also in the issuer and the holder presenting it, effectively mirroring traditional human-vetted verification mechanisms but within a digital framework.

At their core, trust models typically address four foundational questions that define the dynamics of trust in the digital interactions;

- **Who trusts whom?:** identification of the trust relationships among actors such as issuers, holders, and verifiers
- **Why is trust established?:** The underlying justification for trust, whether based on cryptographic assurances i.e., digital signatures, regulatory compliance e.g., eIDAS, social endorsement, or institutional reputation.
- **How is trust evaluated or quantified?:** The use of algorithms, policy rules, or scoring systems to assess the credibility and validity of credentials dynamically.
- **When is trust evaluated or updated?:** Conditions under which trust relationships are re-evaluated, suspended, or terminated, such as through revocation registries or credential expiry[58].

These dimensions collectively enable a granular understanding of trust in complex digital interactions.

Thus, various trust models have emerged to address different trust establishment needs in the digital systems. One of the most established frameworks is the explicit trust models, exemplified by PKI. In such models, trust is hierarchically structured through certificate chains issued and validated by CAs, ensuring a clear and auditable path of trust for secure communication and identity validation via digital signatures and encryption mechanisms[14]. In contrast, Implicit trust models rely on contextual and social cues rather than formal cryptographic validation. These Models assume trust based on prior relationships, endorsements, or reputation, similar to word-of-mouth recommendations or professional references in traditional hiring practices even though they often lack formal verification guarantees[137].

Algorithmic trust models operationalize trust through computational techniques that include reputation, scoring, trust propagation algorithms, or machine learning-based inference. Such models dynamically evaluate the trustworthiness of entities based on behavioral patterns, feedback loops and historical interactions, rendering them particularly useful in highly dynamic, decentralized marketplaces or [93]. In digital employment verification context, these models may enhance the credibility of decentralized issuers or verifiers by incorporating historical performance or institutional reputation.

Policy-based trust models define trust through pre-established access control policies, contextual attributes and compliance requirements. This model is fundamental to Zero-trust architectures, where no entity is inherently trusted and access is continuously verified based on identity, location, device, and role [67]. Within the employment verification context, policy-based trust models are vital in enforcing data minimization, consent management, and compliance with regulatory frameworks such as GDPR and eIDAS.

However, these varying trust paradigms are not mutually exclusive, rather they often coexist within hybrid systems, particularly in SSI and DLT enabled environments. In such ecosystems, explicit cryptographic proofs are complemented by policy-based controls and algorithmic scoring to create robust, interoperable and privacy-preserving trust frameworks that support digital credential exchange at scale[101]. These principals are implemented using Decentralized Identifiers (DID), VCs, and government frameworks like EBSI or ToIP stack. By formalizing trust in this manner, systems can achieve cross-broader interoperability, privacy-preserving verification and resilience against

single point of failures, which is a key requirement in the age of remote work and global talent mobility[140].

4.4 Evolution of the Trust Models

Trust models manifest in different structural and operational forms. Each model reflects distinct assumptions about authority, trust propagation and risk management. The choice of a trust over time has had direct influence on how credentials are handled, issued, and verified, and accepted across stakeholders.

4.4.1 Current Employment Trust Models

The current and contemporary employment verification processes are characterized by significant fragmentation, inefficiency, and reliance on outdated systems, revealing a systematic lack of a cohesive identity layer within the internet's infrastructure. The current trust establishment modes governing employment credentials are typically siloed, exhibiting limited interoperability and automation. This situation imposes considerable technical and operational burdens on verifying entities, which are predominantly hiring organizations. Consequently, these models impose privacy concerns for the individuals undergoing verification process, as their sensitive data can be mishandled or inadequately protected [19].

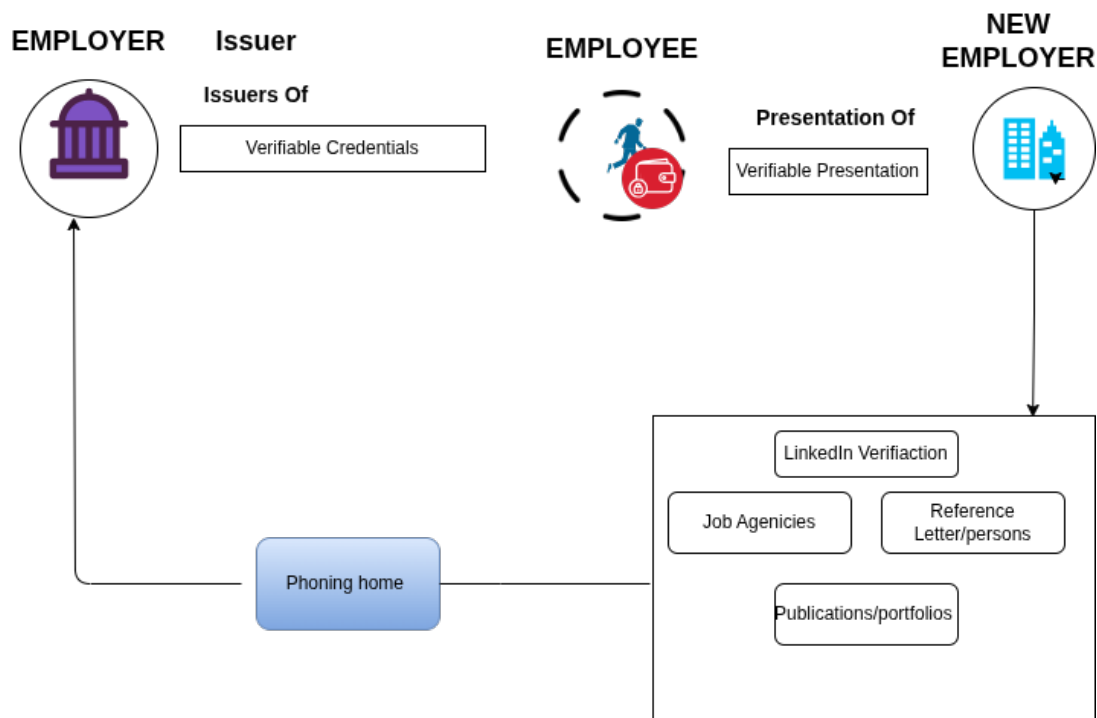


Figure 3: Example Flow of The current Trust Establishment Model

A common method for verifying employment involves direct communication between the prospective employers and former employers (referred to as "Phoning Home") to validate aspects of an applicant's claims such as previous job titles, employment duration and job responsibilities. This verification process is often supplemented by indirect trust signals, such as online profiles on platforms like LinkedIn, data from recruitment agencies, or professional references provided by the candidate themselves as we have highlighted in Section 3.4. These sources serve as abstract verifiable observations, attempting to establish

trust in the absence of a formalized and standardized credentialing framework as depicted in Figure 3 Above[91].

Despite the widespread use, employment verification models face significant challenges. The reliance on manual processes like phone calls and email exchanges introduces delays and a heightened risk of human error, negatively impacting efficiency. Furthermore, third-party intermediaries, including background check firms and credential verification services, complicate the verification landscape, accruing additional cost and operational complexities, especially at scale[182]. The centralized handling of sensitive personal information raises compliance issues under regulations such as GDPR, as these systems become increasingly vulnerable to data breaches. Finally, the lack of automation and standardization leads to inconsistencies and delays in decision-making, significantly hampering the overall effectiveness of the employment verification process[36].

The traditional phoning home model lacks the cryptographic assurances to protect the integrity of the information provided. This exposes verification processes to risk related to data tampering and fabrication, further highlighting the need for more reliable verification mechanisms. Current trust models exemplify employer often engage in laborious external communication channels to authenticate claims, frequently without the benefit of cryptographic validation.

The challenges inherent in contemporary employment verification systems signal an urgent need for the development of improved solutions that prioritize privacy and are cryptographically verifiable. The limitations of the existing frameworks necessitate the exploration of decentralized digital identity models, such as those implemented by blockchain technologies, which seek to reduce the reliance on centralized authorities and manual trust processes. These evolving frameworks offer the potential for standardized, issuer-signed, user-held verifiable credentials, facilitating a transformative shift from phoning home to automated, trustworthy verification systems[91].

In the next section we look into the evolution of these trust models to the point of shift to the digital automated SSI verifiable trust models.

Document-Centric and Centralized Employment Verification Mechanisms

The contemporary employment verification remain predominantly document-centric and are often structured around centralized authority models[163]. Despite notable advances in digital identity technologies the verification of employment credentials particularly in cross-boarder, compliance-sensitive, or legacy-dependent contexts continues to rely on physical artifacts and institutional endorsements as proxies for trust. These practices are deeply embedded across both public and private sector processes, and are widely used in settings where digital infrastructure is either constrained or fragmented.

A qualitative examination of existing hiring documentations and industry procedures reveals a consistent reliance on institution-dependent artifacts for verifying employment history. As outlined in previous sections, these include reference letters, stamped certificates, and signed contracts all bearing organizational branding or symbolic representations of authority. The exploratory insights confirm that such artifacts remain prevalent, especially in international hiring scenarios where manual inspection and institutional familiarity are often the only safeguards against fraud, reference Figure A7 as an example of required proof.

While these methods provide superficial assurances of legitimacy, their practical limitations are substantial. They remain susceptible to forgery, lack machine-readability, and offer limited interoperability across jurisdictions. Furthermore, their verification

often depends on manual intervention, such as contacting issuing organizations directly, introducing delays and inconsistencies that hinder scalability in modern, digitally integrated recruitment ecosystems.

From a theoretical standpoint, effective employment verification must satisfy requirement for authenticity, integrity and timeliness. Yet, conventional paper-based documentation offers no cryptographic guarantees and cannot support automated validation at scale. Based on this premise, it is logically deduced that current verification models are no longer adequate in an environment where trust, speed, and data accuracy are essential to hiring outcomes. These shortcomings provide compelling justification for exploring alternatives that enable an ecosystem like verification of employment claims.

Historical parallels can be drawn to early trust architectures in digital systems, such as IANA and ICANN, which centralized governance over internet infrastructure but also introduced known issues—namely, siloed data, interoperability barriers, and single points of failure [86, 87]. Even modern national identity systems, such as Belgium’s CSAM and itsme platforms, while offering high-assurance onboarding in line with eIDAS standards, still operate under centralized models that face limitations in dynamic, cross-border employment verification use cases [179].

4.4.2 Paradigm Shift; Ecosystems Era

The rapid pace of technological innovation has fundamentally transformed the global operational landscape, particularly within HR. Traditional HR processes, which have long relied on paper-based workflows, face-to-face interactions, and fragmented data storage systems, are being replaced with integrated, automated, and data-centric systems [3], [151] as depicted in 4. The evolution from federated systems to integrated digital ecosystems involves not only technical upgrades but also a reconfiguration of trust, governance, and data ownership paradigms [151], [65]. This shift is driven by the need for enhanced operational efficiency, privacy protection, and interoperability to support globalization and distributed workforces.

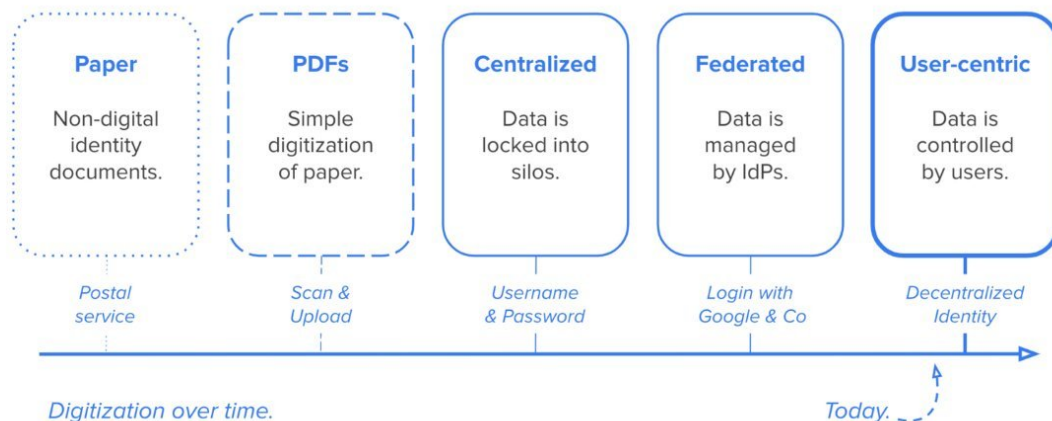


Figure 4: Digital Transformation over time source: <https://walt.id/white-paper/digital-identity>

Historically, manual processes such as recruitment, onboarding, workforce management, and employment verification relied on legacy systems that were sufficient for localized operations but are increasingly inadequate in today’s globalized environment [3]. The limitations inherent to siloed data and fragmented identity systems have accentuated the need for solutions that decentralized control and center

individuals in identity management [46]. Such approaches enable the transfer of control over personal and professional credentials from institutionally managed databases to distributed, user-controlled frameworks thereby promoting reliable cross-organizational interactions[151].

This fundamental shift towards a digital ecosystem marks a departure from merely automating existing processes. Instead, it establishes a new foundation of interoperability, variability, and autonomy by incorporating trust frameworks, decentralized identifiers(DID), and Verifiable Credentials (VC).[151]. For instance, modern HR systems are increasingly adopting Self-Sovereign Identity architectures, which allow individuals to manage, control, and selectively disclose their personal information and high-value credentials, such as academic qualifications and employment history. SSI not only addresses the inefficiencies and vulnerabilities of traditional, centralized approaches but also sets the stage for secure, agile and compliant operational processes.

4.4.3 Self-Sovereign Identities Ecosystem

Self-Sovereign Identity (SSI) represents a transformative approach to digital identity management, prioritizing user control and decentralization[99]. Unlike traditional models, SSI places users at the core of identity administration, allowing them to manage and share their identity credentials autonomously while ensuring privacy and interoperability as depicted in figure 5 below. As outlined in Path to Self-Sovereign Identity [163], SSI builds on the concept of user-centric identity by extending it to ensure that users have full control over their digital identity.

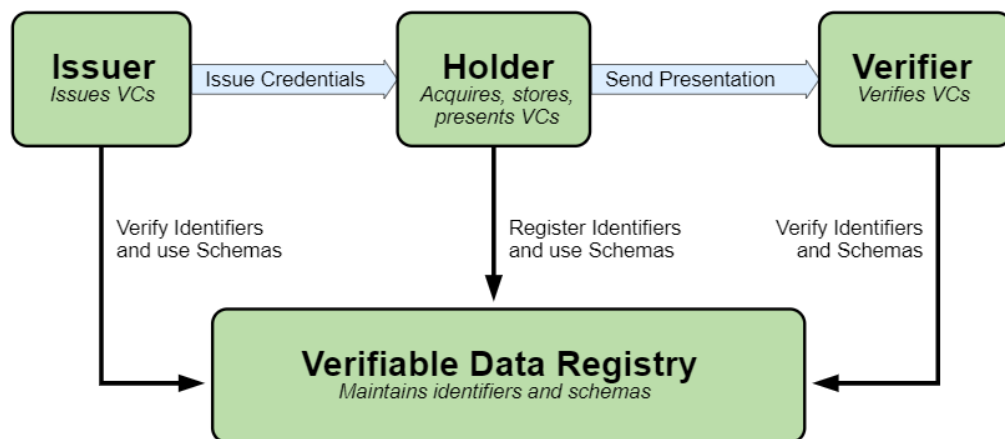


Figure 5: This diagram depicts different components that make up the SSI verifiable credential Ecosystem SOURCE: <https://www.w3.org/TR/vc-data-model-2.0/>

This means, users not only decide when and how their identity is shared but also retain ownership of their credentials. In SSI frameworks, such as those developed by W3C and initiatives like the EBSI, rely on Verifiable Credentials VCs data models to achieve this vision. As, verifiable credential binds user-centered identity to identifiers issued by recognized authorities, such as governments or educational institutions, enabling users to securely prove specific attributes like roles, skills, or certifications—without revealing unnecessary personal information.

Key SSI Entities

The SSI ecosystem operates through interaction among several core entities, each playing a distinct role in the management, issuance and verification of digital credentials [113]. the entities ISSUERS, HOLDERS, and VERIFIERS and the supporting Infrastructure, forming a triangle ensuring the system functions securely and transparently and autonomously.

Issuers:

Issuers are entities that create and issue verifiable credentials to Holders. These credentials serve as attestations of identity attributes, such as a name, qualification, or role, and are cryptographically signed to ensure their authenticity.

Holders:

Holders are individuals or entities who receive, store, and manage their digital credentials. In SSI, the Holder is central to the identity ecosystem, controlling their credentials and deciding when and with whom to share them. Credentials are typically stored in digital wallets, which provide secure mechanisms for managing and presenting credentials.

Verifiers:

Verifiers are entities that request and validate credentials from Holders. They rely on the authenticity of the credentials issued by trusted Issuers to make decisions, such as granting access to a service or verifying eligibility for a program.

Verifiable Data Registry

Support Infrastructure

The infrastructure in SSI systems includes decentralized technologies, open standards, and governance frameworks that enable secure, interoperable, and privacy-preserving interactions among the core entities; issuers, holders, and verifiers. The primary components of this infrastructure include:

1. *Decentralized Identifiers*

DIDs are globally unique, resolvable identifiers that enable entities to establish verifiable, cryptographically secure relationships. They are created and managed by holders, without dependence on centralized authorities. Upon resolution, a DID points to a DID document, which contains metadata such as public keys, service endpoints and authentication methods

2. *verifiable Credentials and Verifiable Presentation*

These are tamper-evident, cryptographically signed digital credentials issued by trusted entities (Issuers) and held by individuals or organizations (Holders). VCs ensure secure data sharing, while VPs allow holders to present selected credential data to verifiers in a context-specific and controlled manner.

3. *Trust Registries*

Many SSI systems utilize DLT, such as blockchains, to maintain immutable records of DIDs, credential schema and governance related data. These registries act as decentralized trust anchors and provide a shared source of truth, reducing reliance on centralized intermediaries.

4. ***Digital Wallets*** They are secure software or hardware-based applications that allow holders to manage their digital identities, including DIDs and credentials. Wallets support cryptographic operations, credential storage and secure presentation of VPs. They are critical for enforcing user control and privacy preferences[46].

5. ***Cryptographic Keys and Public key infrastructure***

The core of identity control in SSI relies on asymmetric cryptography. Public-private key pairs are used for authentication, digital signing, and encryption. Public keys are embedded in DID Documents and shared openly, while private key conveying control are securely stored often within digital wallets. Common cryptographic algorithms include; ed25519, secp256k1, RSA[142].

6. ***Data Exchange Protocols***

These protocols facilitate secure, authenticated and encrypted transmission of verifiable credentials and presentations across the SSI ecosystem. They enabled structured interaction between issuers, holders and verifiers. key protocols include;

- **OpenID Connect for SSI (OIDC4SSI/SIOP):** A self-issued OpenID provider protocol, extending OpenID Connect for decentralized identity authentication and authorization.
- **OpenID for Verifiable Credentials(OpenID4VC):** A suite of specifications form the OpenID foundation designed for the privacy-preserving issuance and presentation of VCs and VPs, compatible with a variety of credential formats and wallet implementations.

5 STATE-OF-THE-ART TECHNOLOGIES

The digital implementation of trust establishment models relies on a set of emerging technologies that provide the infrastructure, assurance and governance mechanisms necessary to evaluate, assert and implement trust across distributed ecosystems. These technologies bridge theoretical trust frameworks with the operational reality, enhance, enabling secure, privacy-preserving and verifiable credential exchange without relying solely on intermediaries.

Thus, this section highlights a list of technologies and frameworks that underpin digital trust models implementation in systems. Each technical tool plays a significant role in the implementation and build up of the entire ecosystem.

5.1 Decentralized Identifier (DID)

A DID is a globally unique, self-sovereign identifier assigned to an entity whether a person, organization, or device. Unlike traditional identities like emails addresses and usernames issued by centralized authorities, A DID are generated and controlled directly by the entity they represent, there eliminating dependence on intermediaries and enhancing autonomy in identity management[38].

In the context of this project, DIDs play a foundational role in enabling secure, verifiable interactions among the primary actors, employers, employee and hiring organizations. Each actor possesses a DID that serves as a secure, resolvable reference point in the credential lifecycle. For instance, when an employer issues a VC to an employee, the credential is anchored to the issuer's DID, allowing any third-party verifier to validate its authenticity through cryptographic proofs.

Key characteristics of DIDs include:

- Is **Unique**, Similar to a uniform resource locator (URL) or phone number, ensuring it points to only one entity.
- Is **decentralized**, meaning it is not issued or maintained by a central registry or intermediary.
- Is **interoperable**, conforming to W3C DID specifications, making it compatible across platforms and ecosystems.
- Is **cryptographically secure**, leveraging public-private key infrastructure to ensure secure interactions and prevent impersonation.
- Is **machine readable**, enabling automated systems to resolve and interpret them via standardized DID Documents.
- Is **verifiable**, allowing recipients to validate the source and integrity of associated data or credentials.
- Is **persistent**, meaning it does not require re-issuance or external validation, even as underlying metadata, or affiliations evolve

They are structured as simple text strings that consist of three parts ; the **did** *URL scheme identifier*, and the *identifier DID method and the DID method-specific identifier* as shown in figure 6



Figure 6: A simple example of a DID, Source:<https://www.w3.org/TR/did-1.0/>

In our context, they form the backbone of digital trust and autonomy, supported by its set of capabilities as mentioned above that enable full lifecycle management. Entities within the employment domain can create their own DIDs in various methods including `did:key`, `did:web`, or `did:ebis`, giving them complete ownership and control over their cryptographic key pairs.

To ensure persistence and auditability, DIDs can be anchored on a distributed ledger, such as the EBSI infrastructure, IOTA's Hyperledger framework Proof of Authority (PoA), making them tamper-evident and consistently available. Through resolution, systems can retrieve associated DID documents that contain essential public keys and service endpoints, enabling interactions with DID subjects[8].

The DIDs have some important properties that are essential in established of an identity and this properties include;

5.1.1 DID Subject

This refers to the entity being referenced by the given DID, i.e., natural persons, organization, device, digital agents, or even abstract concept. They are central to the trust relationships established in decentralized systems as they are the entity whose identity is being asserted, proven or verified.[38]

In the employment verification DID subject would be, the employee whose employment credentials are issued and shared or the employer who issued the employee with a VC. The DID itself provides a unique reference to the employee, while the associated DID Document contains public keys and service endpoints that allow other to verify cryptographic proofs of authority. This proof are used by verifiers like prospective employers to ensure the credentials originated from trusted issuer and pertain to the correct subject without requiring direct access to the issuer.

The self-managed nature of DIDs allows the subject to control multiple identifiers for different purposes, enabling contextual identity separation and minimal disclosure. For example, an individual may use one DID to represent their professional credentials and another for personal interactions, thereby reducing correlation risks across domains [8]. The role of DID subject becomes particularly relevant in trust models that emphasize autonomy, selective disclosure and cryptographic assurance over institutional trust. By shifting control to the subject the DID framework enhances data sovereignty, privacy preservation and trust portability in cross-domain credential verification scenarios.

5.1.2 DID Document

The DID Document serves as a machine-readable document that describes essential information needed to interact securely with the DID subject. According to the W3C DID core specification [23], the DID Document contains public cryptographic resources, verification methods and service endpoints associated with a specific DID[38]. Each DID resolves to a DID Document, which defines how the identifiers can be cryptographically authenticated and how interactions with that entity can be securely performed.

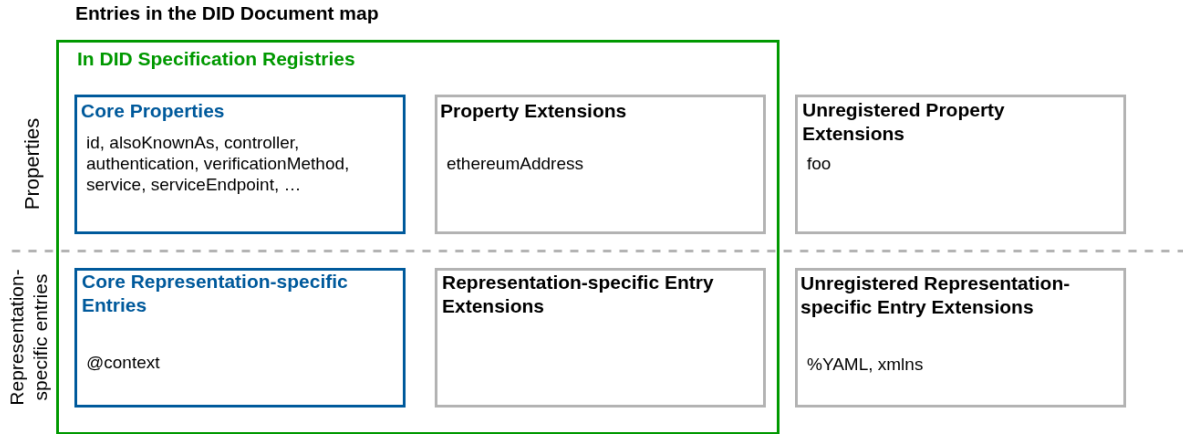


Figure 7: The entries in a DID document, Source: <https://www.w3.org/TR/did-1.1/dfn-did-documents>

As shown in Figure7 Above, the DID Document data model consist of two main classes of entries; The core properties which are required or optimal elements that describe the identity and capabilities of the DID Subject and a Representation-specific entry pertaining to how the DID Document is expressed in specific serialization formats such as JSON, JSON-LD. A representation is a concrete, serialized version of the DID Document.

In our proposed solution DID Documents are consumed and interpreted by the components such as digital wallets, verifiers, and issuer APIs, ensuring that all interactions involving VCs are both cryptographically verifiable and aligned with decentralized trust models.

```
{
  "@context": "https://www.w3.org/ns/did/v1.1",
  "id": "did:example:123",
  "authentication": [
    {
      "id": "did:example:123#z6MkmM42vxfqZQsv4ehtTjFFxQ4sQKS2w6WR7emozFAn5cxu",
      "type": "Multikey", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "z6MkmM42vxfqZQsv4ehtTjFFxQ4sQKS2w6WR7emozFAn5cxu"
    }
  ],
  "capabilityInvocation": [
    {
      "id": "did:example:123#z6Mkvtac9bidSz9bBttzn7Yg3oCDHvMY2FtkFLs6SXRQgdQR",
      "type": "Multikey", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "z6Mkvtac9bidSz9bBttzn7Yg3oCDHvMY2FtkFLs6SXRQgdQR"
    }
  ],
  "capabilityDelegation": [
    {
      "id": "did:example:123#z6MknxsdF4CGVxhRNsx6TvXPfczaHEkajKBBwu75uwBmgpom",
      "type": "Multikey", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "z6MknxsdF4CGVxhRNsx6TvXPfczaHEkajKBBwu75uwBmgpom"
    }
  ],
  "assertionMethod": [
    {
      "id": "did:example:123#z6MkgYhVuWq4hyc7ZKBGhsY7pb5Bc8V6VPXGP63EPja8JBFR",
      "type": "Multikey", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "z6MkgYhVuWq4hyc7ZKBGhsY7pb5Bc8V6VPXGP63EPja8JBFR"
    }
  ]
}
```

Figure 8: An Example of a DID Document

This mechanism allows entities to resolve each other's DID Documents dynamically

and securely, forming the basis for trustless, interoperable identity verification in cross-border and enterprise employment scenarios hence having a document as depicted in Figure 8 Above.

5.1.3 DID Controller

The DID Controller is the entity that has the authority to manage a DID and its associated to DID Document. This control is typically established through possession of private cryptographic keys that correspond to public keys listed in the DID Document [119].

In practice, the controller can perform operations such as updating authentication methods, rotating keys, or changing service endpoints. In decentralized identity systems, the DID controller ensures operational trust by securely managing how the DID evolves over time, see Figure 9 below

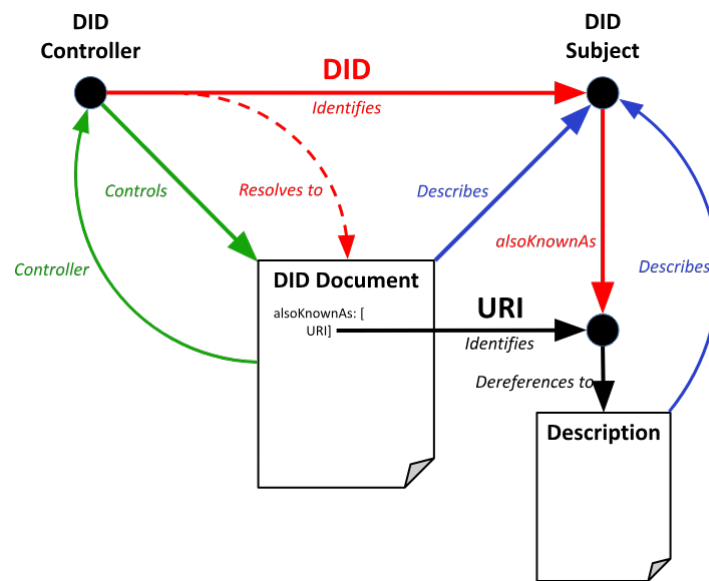


Figure 9: An example depicting a DID Controller Function

in the employment verification the DID controller is often the credential holder, a job applicant who presents verifiable credentials to the issuer, an employer who manages credentials issuance. secure key management by the controller is essential for maintaining credentials integrity, privacy and trustworthiness across ecosystems such as EBSI

5.1.4 DID Resolution, Dereferencing and Method

The interaction between the DID and its associated resources involves the above concepts enabling the retrieval and contextual interpretation of DID related data across distributed networks. The DID resolution is the process which a DID is transformed into its corresponding DID Document using a defined mechanism. This process enables entities such as verifiers and relying parties to obtain metadata about the subject of the DID such as the public keys and service endpoints, which are necessary for verifying digital signatures or establishing secure communications[156].

The DID Dereferencing extends the resolution process by retrieving specific resources referenced within a DID Document, such as verifiable credentials or service endpoint. While resolution returns the entire DID Document, dereferencing targets a

particular element, typically using fragment identifiers or metadata pointers. This supports fine-grained access to credential related information while preserving privacy and minimizing data exposure[138].

The DID Method defines how the specific type of DID is created, updated, deactivated and resolved within a particular ledger or decentralized system. Each DID method includes specification that describes its syntax, supported operations and how resolution is handled within that ecosystem e.g., *did:ebssi*, *did:sov*, *did:key*[78].

5.2 Verifiable Credentials (VCs)

Verifiable credentials are a cryptographically secure and privacy-preserving form of digital credential, designed to represent claims about a subject in a tamper-evident and machine-readable format.[101]. In essence, Verifiable Credentials enable the digital equivalent of traditional paper-based credentials such as academic transcripts, ID cards, or employment records, while supporting cryptographic assurance, selective disclosure and decentralized issuance and verification.

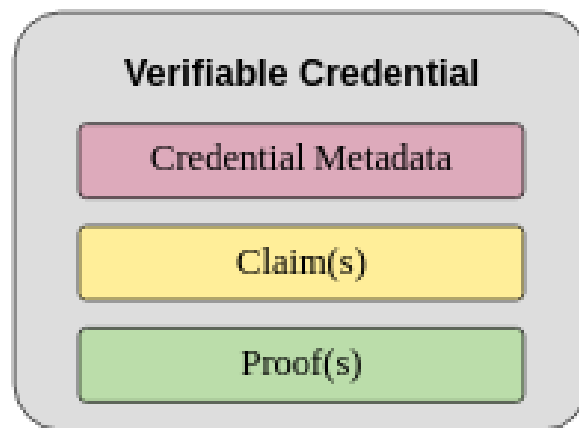


Figure 10: Basic Components of a Verifiable Credential Source: [W3C Verifiable credentials](#)

A credential is then defined as a set of one or more claims made by the same entity, they may include identifier and metadata to describe properties of the credential such as the issuer, the validity data and timestamp, a representative image, status information and any other claim thus forming a verifiable credential as shown in figure A1.

According to the W3C verifiable credentials specification[173], a VC allows Holder of the VC to generate verifiable presentations and then share these presentations with the Verifiers to prove they possess VCs with the specific characteristics in a verifiable format leveraging security and trustworthiness through application of digital signatures. By binding VCs to DID within a DID Document, they ensure a strong association with the specific identity, reinforcing their authenticity and integrity[23].

5.2.1 VC cryptographic Proof Process

VC Data integrity 1.0 describes the mechanisms for ensuring authenticity of VCs through digital signatures and related mathematical proofs. the operations of data integrity is quite simple to create a cryptographic proof you:

1. **Transformation** a process described by transformation algorithm that takes input data and prepares it for hashing process

2. **Hashing** The process by hashing algorithm calculates an identifier for the transformed data using a cryptographic hash function.
3. **Proof Generation** a process described by a proof serialization algorithm that calculates a value that protects the integrity of the input data from modifications or proves a certain desired threshold of trust

the diagram 11 depicts how the cryptographic proof is created



Figure 11: View of the proof generation Steps, Source:<https://www.w3.org/TR/vc-overview/proof-generation-steps-figure>

5.2.2 Verifiable Presentation

In W3C VC data model, Verifiable Presentation(VP) is a tamper-evident cryptographically verifiable data structure that enables a holder to present credentials to a verifier in a secure manner[174]. While VC provide the underlying claims issued by trusted entities, the VP acts as the transportation mechanism through which those credentials or selected subsets of them are shared during interactions.

```

{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "type": ["VerifiablePresentation"],
  "verifiableCredential": [
    {
      "@context": ["https://www.w3.org/2018/credentials/v1"],
      "type": ["VerifiableCredential", "EmploymentCredential"],
      "issuer": "did:web:robskytec.local",
      "issuanceDate": "2025-03-01T10:00:00Z",
      "credentialSubject": {
        "id": "did:key:z6MksJaneDoe",
        "jobTitle": "Software Engineer",
        "employer": "Robskytec Limited"
      },
      "proof": {
        "type": "Ed25519Signature2020",
        "created": "2025-03-01T10:01:00Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod": "did:web:robskytec.local#key-1",
        "jws": "eyJhbGciOiJIJZERTQSi99..sig"
      }
    }
  ],
  "holder": "did:key:z6MksJaneDoe",
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2025-05-29T11:45:00Z",
    "proofPurpose": "authentication",
    "verificationMethod": "did:key:z6MksJaneDoe#key-1",
    "challenge": "random-challenge-id",
    "domain": "verifier.example.org",
    "jws": "eyJhbGciOiJIJZERTQSi99..holdersig"
  }
}

```

Figure 12: An Example of Verifiable Presentation showing the Presentation verification process

VPs may include one or more VCs, along with metadata and a cryptographic proof that binds the presentation to the presenter. This binding is important for establishing the authenticity of the presenter and ensuring that the data has not been altered in transit. The structure of a VP often include:

- **@content:** This links the presentation to one or more semantic vocabularies
- **type:** Typically includes the Verifiable Presentation to indicate compliance with the VC model.
- **Verifiable Credential:** A list of one or more credentials being presented.
- **Holder:** The Decentralized identifier of the entity presenting the credential.
- **Proof:** A cryptographic proof like digital signature or zero-knowledge proof used to verifying the authenticity and integrity of the presentation .

5.3 Digital Wallets

Digital wallets serve as secure, user-centric containers for the management, storage, and controlled disclosure of digital identity artifacts, including DIDs, VCS and VPs. Within the context of European Digital Identity (EUDI) framework, the digital wallet is an important trust-enhancing component that enables end users (natural or legal persons) to interact securely and privately with the issuers and verifiers in digital credential ecosystems [88]. Functionally, digital wallets offer the following core capabilities;

- **Credential storage and Management** The wallet acts as a persistent, secure repository for one or more VCs. These credentials may be issued by trusted entities and are stored locally or in encrypted form accessible to the holder.
- **Presentation control and Selective Disclosure** Users maintain full control over when and how credentials are shared. Wallets enable selective disclosure where only specific claims within a credential are revealed using cryptographic techniques such as ZKP.
- **Cryptographic key management** Wallets manage private keys associated with DIDs and verifiable credentials. This allows the holder to produce verifiable presentations and signatures, proving control of the credential while ensuring non-repudiation and integrity.
- **User Authentication and Consent:** Wallets incorporate strong authentication like biometric, PIN-based, or hardware-backed mechanism to prevent unauthorized access. Additionally any credential sharing or data transfer operations must be explicitly consented to by the wallet holder, ensuring compliance with the user-centric data governance models

According to the EUDI Architecture and Reference Framework [53], digital wallets are categorized into wallet providers and credential providers, with well defined interfaces and protocols for secure credential issuance, storage and verification. The EUDI wallets also defines interoperability catalogues that allow wallets to interoperate across borders and domains by specifying standardized credential types, assurance levels and trust registries [54].

Importantly wallets also support multi-credential orchestration, allowing for bundling of credentials from multiple issuers into coherent, purpose-driven verifiable

presentations. This is particularly valuable in scenarios such as cross-boarder employment verification, where credentials from educations, professional licensing and prior employment history must be harmonized and verified by a third party[159].

5.4 OpenID4VC

OpenID for Verifiable Credentials is an emerging set of protocols developed by the OpenID Foundation to facilitate secure, interoperable, and privacy preserving exchange of verifiable credentials and verifiable presentations across diverse ecosystems. Building on the robust security foundations of OpenID Connect and OAuth 2.0, OpenID4VC enables credential issuers, holders and verifiers to interact seamlessly using well established web standards while accommodating the decentralized trust models inherent in SSI architectures.

It introduces two primary protocol families

- **OpenID4VCI (credential Issuance):** Enables a holder to obtain verifiable credentials from an issuer using the standard OAuth-like flows. This includes dynamic credential offers, token-based access authorization and credential formats agnostic to ecosystems
- **OpenID4VP (verifiable Presentation):** Allows holders to present credential in privacy preserving and verifiable manner Supporting Selective disclosure, audience binding and replay protection, ensuring that only the necessary claims are shared.

In practice, OpenID4VC is designed for seamless integration with digital wallets allowing credential holders operate without relying on centralized intermediaries: Within the EUDI, the ARF identifies OpenID4VC as a preferred protocol for credential life cycle management due to its scalability, modularity, and alignment with the decentralized trust principles[89].

5.5 JSON-LD

JSON-LD (JavaScript Object Notation for Linked Data) is a lightweight and flexible data interchange format designed to represent linked data in a way that is easy to read, write, and process. It builds upon JSON, adding semantic context to the data, making it a key technology in the development of decentralized identity systems and verifiable credentials (VCs). JSON-LD adheres to the W3C standards, making it highly interoperable for decentralized and web-based ecosystems.

5.6 SD-JWT

Selective Disclosure JSON Web Token (SD-JWT) is an extension of the traditional JWT (JSON Web Token) designed to enable selective disclosure of claims within a credential or token. Unlike standard JWTs, which disclose all embedded claims when shared, SD-JWT introduces mechanisms for sharing only the necessary claims while keeping other data private. This feature is particularly valuable for privacy-preserving applications, such as verifiable credentials and decentralized identity systems.

5.7 Git and Git Hub

Git is a distributed version control system designed to track changes in source code during software development. It enables multiple developers to collaborate efficiently by

creating a history of changes, supporting branching, merging, and rollback functionalities. Git ensures that project files are synchronized and any modifications can be managed systematically.

GitHub, built on Git, is a web-based platform for hosting and managing Git repositories. It adds collaborative tools, such as pull requests, issue tracking, and workflows, to enhance team productivity. GitHub also integrates features like versioned backups, CI/CD pipelines, and community engagement through open-source projects.

Together, Git and GitHub streamline development workflows, facilitate version control, and foster collaborative software creation in an organized and transparent environment.

5.8 Postman

Postman serves as a state-of-the-art API development and testing tool that has garnered significant traction in the software industry. Launched as a REST client, It has evolved into a comprehensive platform that supports the entire API lifecycle, including management, testing and automation, across various protocols such as REST, GraphQL and gRPC. This evolution reflects the broader industry trend towards API-first design methodologies, as highlighted in the growing preference for design-oriented approaches that facilitate stakeholders communication around AS specifications. In decentralized identity systems specifically, where operations such as credential exchange hinge upon the reliable API interactions, Postman offers a robust environment for testing and validating these interactions.

- **Endpoint Exploitation and Debugging:** Instrumental in testing critical RESTful API endpoints, including those associated with creating DIDs and managing VCs issuance and verification processes. Through comprehensive endpoint exploration capabilities, the tool allowed us to ensure that the responses to credential requests, particularly those formatted as JSON Web Token and Linked Data verifiable Credentials.
- **Authentication and Security Header Testing:** given the sensitive nature of the data involved in decentralized identity systems, robust authentication mechanisms are crucial. Postman enables simulation of OpenID Connect flows to evaluate the security of our endpoint effectively.
- **Data payload Validation:** The tool facilitated the crafting and sending of JSON-LD payloads, allowing for comprehensive validation of VPs to support interoperability across various micro-services involved in credential issuance, holding and verification: this capability was essential for assessing the adherence of our data structures to the relevant standards outlined in W3C and EBSI.
- **Automation and Regression testing:** Postman's collection of features allow to automate testing workflows by leveraging environment variables and scripting functionalities. This automation streamlines testing processes across different stages of development, staging and production and ensured a comprehensive regression testing mechanism were in place to rapidly verify schema conformance as iterations of the API evolved.

6 ENABLING ORGANIZATIONS and FRAMEWORKS

6.1 World wide Web Consortium Standards

The world wide web (WWW) Consortium represents a leading international standards organization dedicated to promoting web interoperability and the long-term growth of web technologies. Its commitment to developing open protocols and guidelines has been pivotal in shaping numerous specifications that underpin contemporary internet usage, particularly in the domain of SSI ecosystems. Among its significant contributions are the Verifiable Credential Data Model 2.0 (VCDM 2.0) and DIDs standards, both essential for building robust decentralized identity systems that prioritize user privacy and data ownership [127].

In context of our project implementation adhering to W3C standards provides crucial technical frameworks. The use of VCs enables the formalization of employment attestations in a manner that is tamper-evident and interoperable. This not only enhances the integrity of employment documents but also facilitates easier verification by employers and institutions, mitigating the risks associated with fraudulent claims. Furthermore, the adoption of DIDs allows entities to establish identifiers that are globally resolvable without reliance on centralized registries, thus ensuring enhanced privacy and security in data management [127].

The implementation process involves utilizing W3C VCDM 2.0 and DID core specifications, which provide guidance for the structure and logic of issuance and verification of employment credentials. This project architecture integrates W3C-Complaint models through various services to construct and issue credentials effectively. The representation and resolution of DIDs, particularly utilizing EBSI-compatible methods, further bolster the system's credibility and operational efficacy [66]. Moreover, the ability to verify credentials and presentations using standardized formats such as JSON-LD or JSON Web Tokens (JWT) enhances interoperability across different SSI frameworks, enabling seamless integration with technologies that comply with W3C guidelines.

In a nutshell, the W3C's role in providing normative specifications for decentralized identity systems is indispensable. It fosters compatibility, transparency and trustworthiness within identity verification processes, ultimately facilitating a legally interoperable ecosystem essential for cross-boarder employment verification.

6.2 European Blockchain Services Infrastructure

The EBSI represents significant efforts by the European Union to create a blockchain-based digital infrastructure for the public sector. It is initiated under the European Blockchain Partnership (EBP), EBSI is designed to enhance public services by providing secure, transparent and efficient mechanisms for data sharing and verification. This initiative supports cross-border use cases such as verifiable credentials, digital identities and public administration interoperability with applications for citizens, EU institutions and national governments.

EBSI operates as a public, permissioned blockchain network, where only authorized nodes operated by EU member states and associated parties can participate, its architecture includes

- **Multiple Deployment Environments:**

where development, test, conformance are hosted by the European Commission and the pilot, pre-production and production are managed by the member states

- **Node Types**

Validator nodes: are for proposing and validate blocks using a PoA mechanism

Regular Nodes: which maintain ledger copies and handle network synchronization.

- **Consensus Mechanism:**

EBSI employs a low-energy PoA approach, ensuring efficiency while maintaining data trustworthiness.

- **Integration with Hyperledger Besu**

By utilizing Hyperledger Besu, EBSI ensures compatibility with Ethereum Virtual Machine (EVM)-based smart contracts, fostering adaptability and interoperability.

EBSI embodies the EU's vision for a digitally connected economy, where blockchain serves as the backbone for trust and security. By eliminating intermediaries and automating complex verification processes, EBSI reduces administrative burdens and enhances the user experience. Its alignment with GDPR and other regulatory frameworks further underscores its commitment to privacy and compliance. having these core features and capabilities;

- **Interoperability:**

Built on open standards, EBSI integrates with existing frameworks such as eIDAS, ensuring seamless cross-border digital identity verification.

Supports Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to enable secure, privacy-preserving exchanges of information.

- **Data Security and Privacy:**

Implements robust cryptographic mechanisms to safeguard sensitive data.

Combines restricted write access with public read access, ensuring transparency while maintaining data integrity.

- **Smart Contract Support:**

Allows public sector entities to create automated workflows for use cases such as credential issuance and verification.

- **Decentralized Governance:**

EBSI's governance structure ensures equitable participation from all EU Member States, fostering trust and collaboration among stakeholders.

6.3 European Digital identity Wallet

Europe's identity landscape has transitioned from a federated model under the original eIDAS Regulation (Regulation (EU) No 910/2014) to more user-centric approaches. The federated model required each Member State to issue formal identifiers to its nationals, with mutual recognition across borders. While functional, this system saw limited adoption due to its complexity and lack of flexibility [43].

To address these limitations, eIDAS 2.0 (COM/2021/281 final) proposes the introduction of an EU Digital Identity Wallet[54]. This wallet integrates the principles of SSI by allowing users to store and manage not only their EU Digital Identity but also attributes and credentials issued by different authorities [148]. For example, a user could share role-specific credentials such as employment details or skills instead of their

full identity when accessing services, thus enhancing privacy and minimizing unnecessary data disclosure.

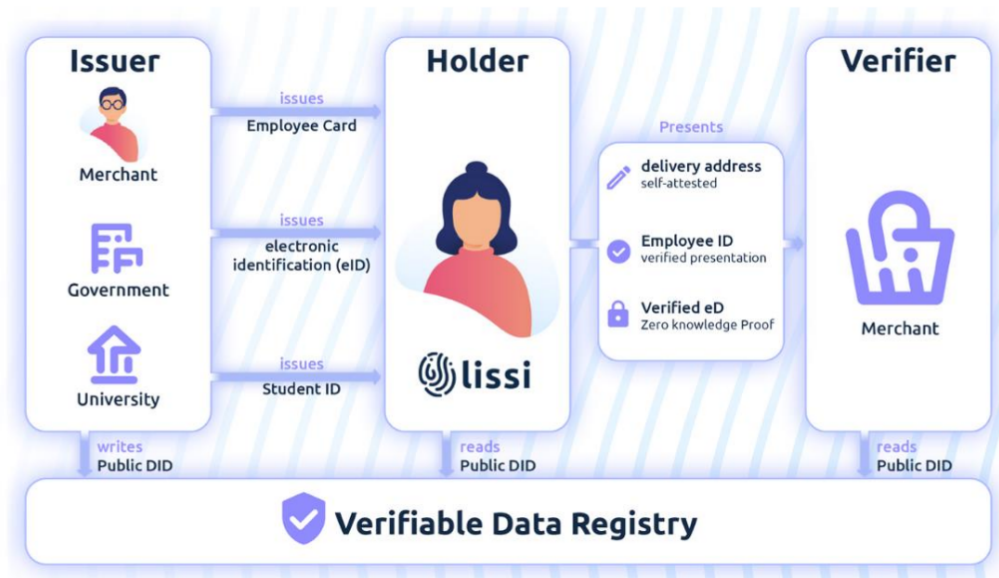


Figure 13: "Digital Identity: Leveraging the SSI Concept to Build Trust" ENISA report, Jan. 2022 <https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-SSI-concept-to-build-trust>

The EUDI wallet plays a pivotal role in fostering a secure and structured digital identity ecosystem within the EU. This initiative stems from the revised eIDAS 2.0 Regulation, which is instrumental in empowering citizens, residents, and businesses across the EU with a sovereign, standardized, and cross-border digital identity solutions. The EUDI wallet ensures that users can securely store, manage and share their Personally Identifiable Information (PII), Electronic Attestations of Attributes (EAA), Qualified Electronic Attestations of Attributes (QEAs), and Qualified Electronic Signatures (QES) in a manner that respects privacy and fosters trust among the users and various stakeholders. The intention behind the EUDI wallet is to enhance interoperability across Member states while establishing a robust Digital identity Framework, essential for promoting cross-border digital services.

The architecture of the EUDI wallet emphasizes a modular and layered system that includes various core services. These services consist of wallet Application Layer allowing intuitive user interaction, wallet core services that handle credential storage and issuance, and an interoperability layer that employs standards such as W3C verifiable Credentials. The presence of Governance services ensure compliance with national regulations and the maintenance of trust registries, which further strengthens the overall ecosystem.

6.4 Linux Foundation

The Linux Foundation plays a pivotal role in the development and promotion of decentralized identity solutions through the facilitation of open-source projects and standards that underpin SSI and DLT systems. By adhering to a neutral, multi-stakeholder governance model, the Linux Foundation encourages collaboration among industries and government to develop common frameworks for digital interactions in an increasingly decentralized world.

One notable initiative is the ToIP, which defines a layered architecture that combines cryptographic elements such as DIDs, Keys, and ledgers with human and legal governance layers to create a comprehensive trust stack[37]. This strategic approach enhances the technical aspects of the digital trust while ensuring that legal and governance model structures align with technological advancements[35]. Consequently open governance model accelerates the adoption of interoperable identity standards like W3C Decentralized identifiers and verifiable credentials across various sectors.

The initiatives led by the LF, such as hyperledger Aries, Indy and Besu, are actively contributing to this landscape by providing reference implementations of these defining standards. hyperledger Aries, for instance, serves as an interoperable SSI framework, facilitating the secure issuance, storage and presentation of VCs. Similarly, Hyperledger Besu is an enterprise Ethereum client that supports PoA consensus mechanisms, thereby broadening the range of middleware solutions available for identity management. These projects effectively equip the developers with the tools necessary to implement credential exchanges and trust registries transparently, in alignment with established standards.

The LF's promotion of open-source code, transparent project roadmaps, and inclusive governance ensures that digital identity frameworks are rigorously vetted and developed collaboratively, thereby aligning technological advancements with the emerging regulatory requirements and trust mandates. By hosting influential projects like ToIP Foundation, the LF emphasizes cross-industry cooperation among diverse stakeholders, including banks, governmental bodies, and NGOs, enhancing the usability and effectiveness of decentralized identity solutions.

Moreover, It fosters board community engagement in the development of digital identity technologies. The trust Over IP foundation convenes working groups that address both technical and governance challenges associated with digital trust. This collaboration leads to creation of tools and libraries that organizations can adopt to develop interoperable SSI wallets and issuers.

6.5 OpenID Connect Foundation

The OpenID Foundation plays a role in shaping the standards that underpin identity interoperability and secure data exchange across digital ecosystems. As the steward of the widely adopted OpenID Connect protocol which extends OAuth 2.0 to support federated identity. It has become a key enabler in bridging traditional authentication flows with emerging decentralized identity models. In the context of our project, the relevance of the OpenID Foundation is particularly evident in the OIDC for verifiable Presentations and OIDC for VC Issuance specifications.

These specifications provide mechanisms for the integrating VCs and DIDs into standardized, interoperable workflows using familiar OIDC protocols. For Example, during the credential presentation phase in our employment verification system, verifier can initiate a credential request through an OIDC-compliant flow, and the holder can respond using their digital wallet, transmitting a cryptographically signed VP.

By aligning with the work of the OpenID Foundation, our system benefits from broad compatibility, and adheres to best practices in secure identity exchange. The OpenID Foundation's Efforts help standardize the adoption of decentralized identity components in real-world use cases, making it a crucial enabler of the trust architecture underpinning the project's verifiable employment ecosystem.

6.6 Walt.id Framework

Walt.id is an advanced open-sourced technology platform specializing in robust building of end-to-end decentralized identity and wallet infrastructure solutions across industries and ecosystems. It provides a comprehensive suite of tools for identity management and governance, enabling organizations to securely issue, manage and verify digital credentials. It acts as an abstraction layer that hides technical complexity and handles different building blocks like trust registries, credential types, and data exchange protocols while ensuring compliance and interoperability.

It is perfectly suited for industries where trust, security and compliance are critical, including employment verification, financial services and healthcare thus enabling a proper Use Case for our project. Its architecture can be broadly categorized into multi-platform libraries, services and Application Programming Interfaces (APIs), applications and external services and integrations making its capabilities align perfectly with the needs of modern employment verification systems with SSI. Its main functionalities include:

- **Streamlined Verification:** Employers can issue verifiable credentials that detail an employee's tenure, role and achievements and these credentials can be securely shared with future employers without intermediaries coming into play.
- **Cross-border Trust:** Walt.id's adherence to international standards makes it suitable for cross-border employment scenarios, reducing friction in verifying credentials across jurisdictions.
- **Automation and efficiency:** By automating credential issuance and verification, Walt.id reduces administrative overhead while enhancing accuracy and trust

The multi platform libraries are based on Kotlin/JAVA, they bring support to variety of programming languages including Kotlin/Java, JavaScript and more. allowing mix and matching of identities features, credentials formats and ecosystems functions to ensure a compact and concise code-base.

- **Core libraries**

1. Crypto: Manages keypair and signature functionalities
2. SD-JWT: Issues Selective Disclosure JSON-Web Tokens.
3. DID: Manages Decentralized Identifiers.
4. OpenID4VC: Facilitates protocol issuance and verification

Also its credential Libraries facilitate the issuance and verification of World Wide Web Consortium (W3C) Verifiable Credentials with various signature formats JWT, Selective Disclosure JSON Web Token (SD-JWT), JavaScript Object Notation for Linked Data (JSON-LD) and support mdoc credentials like mobile driver licenses (mDL). The Ecosystem Libraries provide specific functionalities for operations within ecosystems such as EBSI, cheqd, eIDAS, and IOTA, ensuring compatibility across decentralized identity frameworks.

The platform also features robust Services and APIs to enhance applications with issuer, verifier, and wallet capabilities. The Issuer API enables the issuance of credentials and tokens across ecosystems, while the Verifier API supports credential verification based on customizable policies. Additionally, the Wallet API provides identity wallet functionalities for storing, managing, and sharing credentials and tokens.

To streamline implementation and market deployment, Walt.id includes customizable white-label Applications, such as a Web Issuer, Web Verifier, and a custodial web wallet. These applications support protocols like OIDC4VC and operate as progressive web apps (PWA), ensuring device compatibility. The platform also offers a Command Line Interface (CLI) for developers to experiment with features and manage services directly from the terminal.

Interoperability with third-party services is another strength of Walt.id. It integrates with KMS/Hardware Keystores, Trust Registries, and TSP Signature providers, while also supporting various data storage solutions. This openness allows developers to extend the platform by integrating additional tools for key storage, trust services, and identity verification.

6.7 Internet Engineering Task Force(IETF)

This is one of the most influential organization in the development of open internet standards, particularly those related to secure communication, data exchange, identity protocols. Within the context of this employment verification, the IETF contributes essential protocols and specifications that underpin secure and interoperable identity interactions, many of which are utilized directly or as extended in SSI.

Key IETF developed technologies such as OAuth 2.0, JSON Web Signatures, and CBOR Object Signing and Encryption are directly used or referenced in VC formats, DID resolution mechanisms, and wallet-to-verifier interactions. For instance, the JWT and JWS standards are commonly used in VC implementation to represent and sign credentials in a compact tamper-evident manner. Additionally, emerging extensions such as OAuth2.1 and ongoing work on secure credential exchange protocols provide a foundational layer upon which OIDC4VP and OIDC4VCI build bridging traditional and decentralized authentication paradigms.

By adopting standards rooted in the IETF ecosystem, we ensure cryptographic integrity, transport security, and compatibility with widely accepted digital identity infrastructure.

6.8 Trust Over IP Foundation

This Foundation is a key enabling body that provides a comprehensive governance and technical framework for building interoperable, scalable, and trustworthy digital identity ecosystems. Operating under the Linux Foundation, ToIP promotes a four-layer trust model spanning from technical infrastructure to human trust frameworks—that enables secure, decentralized interactions between entities without the need for centralized intermediaries. This layered model is highly aligned with the objectives of our employment verification project, which seeks to implement a decentralized, standards-based system for issuing and verifying employment credentials.

The ToIP framework offers a structured way to integrate DIDs, Verifiable Credentials (VCs), and Self-Sovereign Identity (SSI) in a manner that supports both technical trust and governance trust via policies, legal agreements, and credential schemas. Specifically, the ToIP model helps define trust assurance levels between issuers, holders, and verifiers, enabling consistent validation of employment history across sectors and jurisdictions.

By adopting principles advocated by the ToIP Foundation such as decentralized governance, credential interoperability, and layered trust separation we ensure that the employment verification system is not only technically sound but also socially and legally credible.

7 ANALYSIS

This chapter builds on the foundations laid in the previous chapters by moving from an understanding of the CV structure and the hiring process toward a critical analysis of how traditional CV claims can be translated into Verifiable Credentials. Section 3.4 deconstructed the CV into its key components, while section 3.2.1 examined how these elements are used and verified in real-world hiring practices. Together, they revealed the trust limitations of the current document-based methods and the potential of decentralized approaches.

This chapter does not attempt to replace the CV in its entirety, but rather we analyse the most verifiable, impactful, and recurrent elements, those which are essential for decision-making in hiring context and explore how they can be digitally represented, issued, and verified in a decentralized manner. This aligns directly with our central research question: How can a decentralised trust framework, incorporating SSI and DLT technologies be applied to support the partial automation of employment verification process, particularly in relation to CV data while enhancing trust and efficiency in the hiring process?

The analysis addresses key problem areas, like establishing trust between the employer and the employee, validating the authenticity of presented credentials, determining which CV claims can be effectively credentialized, and exploring the role of existing initiatives like EBSI in enabling adoption. Components are mapped to potential VC types and classified by trust level, highlighting which may require high-assurance issuers and which can be managed in a low-trust decentralized manner. We also consider how these credentials can integrate with existing digital identity ecosystems to create a complete Verifiable ecosystem.

Finally we reflect on the technical and regulatory considerations required to implement such as system covering privacy, interoperability, and legal compliance, and introduce workflows and scenarios that illustrate real-world credential exchange using the technologies discussed in 5. This insights form the basis for the system design in the next chapter.

7.1 Mapping CV Components to Verifiable Credentials

In the context of our system, this section maps the components of the traditional CV to potential Verifiable Credential types. This mapping takes into account both the level of trust required for each credential and the type of issuer capable of supplying that information in a verifiable, digitally signed format.

While the system proposed is capable of handling a variety of credential types, our scope focuses primarily on low trust credentials, those that can be issued directly by employers or affiliated entities without requiring state-level regulatory oversight. However, it is important to acknowledge that several high trust credentials, such as national identity documents or accredited academic degrees, are essential components of a full verifiable identity. These can be incorporated by forming ecosystem integrations with established SSI frameworks, thereby enhancing their reliability of the overall verifiable agent.

The Mapping in Table 1 below reflects this two-tier trust approach each credential:

Table 1: Mapping of CV Components to Verifiable Credentials

CV Component	Suggested VC Type	Issuer Type	Trust Level	External Ecosystem Support
Personal Information	NaturalPersonID/eID VC	Government ID provider, eIDAS authority	High	eIDAS, CSAM, itsme, NemID/MitID
Educational Background	Educational VC	Accredited university or college	High	Europass, EBSI, university registries
Employment History	EmploymentCredential VC	Employer (HR dept)	Low	LinkedIn pilot programs, internal HR systems
Certifications & Licenses	KYC/ VC	Professional body, training org	High	AWS, PMI, medical boards
Skills & Competencies	EmploymentCredential VC	Employer, team lead, training platform	Low	LinkedIn Skill Assessments, Coursera
References & Endorsements	EmploymentCredential VC	Past manager, academic supervisor	Low	LinkedIn Recommendations
Portfolios & Projects	Project Credential, Portfolio VC	Client, supervisor, self-attested	Low	GitHub, Behance, freelance platforms
Publications	Authorship VC	Journal, publisher, research org	High	ORCID, Crossref, publisher DIDs

However given the legal and institutional authority available to the credential issuers within our scope i.e internal HR departments, supervisors, training coordinators, our system will prioritize low-trust but high relevance credentials. These are sufficient to address the common requirements in employment verification, particularly for early-stage screening, internal HR processes, remote works, freelance or contract-based hiring scenarios.

Nonetheless, by designing our system to be interoperable with external high-trust credential ecosystems, we ensure extensibility. For example, an applicant could supplement their employment related VCs issued by an SME in our system with a digitally verifiable degree issued by a university via Europass or EBSI, forming a composite trust profile validated across domains.

This layered approach supports the development of verifiable agent platform that is modular and scalable, allowing for varying degrees of trust depending on the context industry, and verification requirements. In the next section, we explore how trust levels relate to issuer qualification and governance within a decentralized ecosystem

7.2 Trust Models and Issuer Classification In Employment Verification System.

As part of our endeavour to Establish a solution for our system. We acknowledge that the credibility of VCs in any decentralized systems depends not only on the content of the credential but also the trustworthiness of the issuer. In this context, the trust models, high-trust vs low-trust credentials and their issuer classification intersect to define how credential are issued, validated and accepted.

At the core of this intersection, there is an understanding that not all credentials require the same level of assurance, nor do all issuers operate under the same level of governance. Some credentials for example, academic degrees or national identity documents require issuance by highly qualified, legally recognized authorities that act as anchors to them. Other's such as employment details attestations or role attestations,

can be issued by non-regulated organizations the employee is attached to, relying more on the institutional or reputational trust. Thus we explore this two classes of trust in more detail, providing more context to the credential types, issuer profiles, and verification mechanisms within the broader Employment verifiable ecosystem.

7.2.1 High-Trust Credentials and Qualified Trust Service Provider

In the context of this system, high-trust credentials refer to CV components that require issuance by formally recognized institutions whose legitimacy is grounded in law, regulation, or official governance framework. These credentials are identified in the Table 1, with trust level of High.

These Components, while commonly referenced in traditional CVs as printed or scanned documents, must in a decentralized architecture be transferred into cryptographically verifiable credentials issued by Qualified Trust Service Providers (QTSPs)[142]. The system acknowledges that such high trust credentials lie beyond the operational control of employers or organizations acting independently and instead depend on integration with external, formally on boarded issuers.

To address this, the system aligns with the EBSI trust model, which provides a top-down, policy driven trust architecture rooted in the principles of the eIDAS Regulation (regulation (EU) No 910/214)[133]. EBSI's model operationalizes trust through federated onboarding of credential issuers, such as accredited universities, government agencies, and professional regulators whose legitimacy is published and maintained via national trusted list. These trusted lists serve as legal assurance mechanisms that verifiers across EU jurisdictions can rely on without the need for direct bilateral agreements[168]. Each issuer within EBSI is, first registered through national authorities, listed on a trusted registry, then associated with cryptographic keys bound to their DID and then lastly, they are authorized to issue VCs whose provenance can be validated on-chain.

The system supports credential exchange without requiring verifiers to manually assess issuer authenticity. For example, a verifier reviewing a digitally signed degree credential can resolve the issuer's DID and confirm its presence on the EBSI trusted list ensuring the credentials are both valid and legally recognized[49].

Within the scope of our project, such high trust credentials are not issued directly by the system but are referenced and integrated. The system architecture supports the ingestion and verification of high trust credentials from external ecosystem such as; Educational credentials issued via EBSI's Educational credential Framework, Legal identity documents issued by national digital ID providers MitID in Denmark, and Professional licenses issued by boards listed under national QTSP directories[161]. These high-assurance credentials strengthen the verifiable identity profile of employment subject and form a trust backbone when layered alongside low-trust credentials issued by employers or supervisors.

These the two most suitable types of issuers for these credentials following the EUDI wallet architecture[53] are depicted in Figure

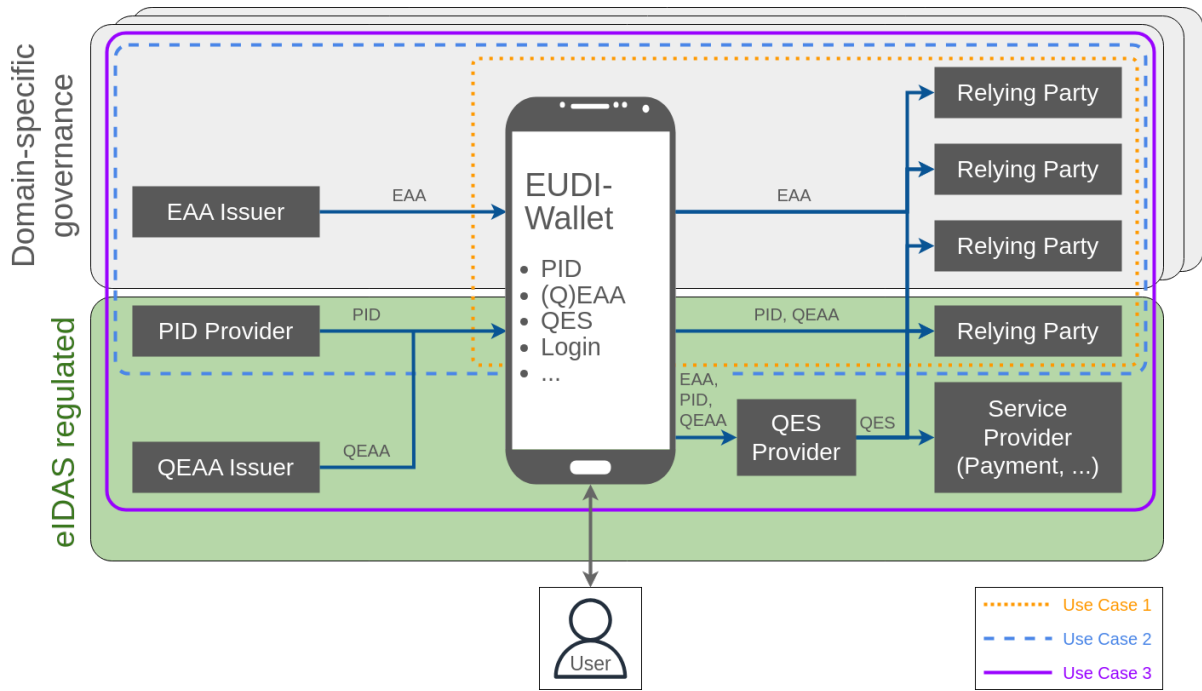


Figure 14: EUDI wallet architecture framework Source: <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/>

• Personal identification Data

PID providers issue fundamental identity credentials such as eIDs, passports, digital identity cards issued by public authorities and legally binding with their identity attributes such as date of birth, name and Nationality[176]. These credentials represent a person's civil identity and serve as the root of trust in as illustrated the EUDI wallet ecosystem in the Figure 14, anchoring all other VCs including those used for employment verification. As legally mandated issuers, PID providers are recognized under the eIDAS regulation and must ensure cross-border interoperability of digital identities within the EU. Their credentials are high-assurance and meet level of Assurance requirements, making them essential for verifying the legitimacy of holders in decentralized systems[53]. In EBSI, these providers function as trust anchors that initiate the trust chain by binding the user's digital identity via a DID to a verified legal identity.

In our architectural implementation, PID credentials would play a vital role during the onboarding and proof presentation. A user must first establish their identity via a PID credential issued by a trusted national authority before claiming or presenting employment-related VCs[13]. This linkage ensures authenticity and legal recognition across member states. For an example, a job applicant presenting a proof-of-employment VC from a foreign employer can be reliably identified by the receiving institution through their PID credential, facilitating trust in transnational hiring scenarios.

• QEAA Issuers (Qualified Electronic Attestation of Attributes)

Qualified Electronic Attestations of Attributes (QEAA) are a new class of credentials introduced by the eIDAS2 regulation for high-trust, regulated use cases. A QEAA is essentially an EAA that is elevated to a qualified status meaning it's issued

by a Qualified Trust service Provider under stringent requirements, giving it the equivalent level effect as paper-based attestations[53]. These are digital counterparts to certified documents or licenses that traditionally would carry legal weight like notarized papers, official certificates, or documents with an official seal. Only issuers who have been granted qualified status by a national supervisory authority can issue them out.

Credentials that are expected to be issued as QEAA's include; civil status document such as birth certificates, professional licenses e.g license to practice medicine or law, certifications of good conduct, company registration certificates etc... in our context these might come into play for roles that require a licensed qualification like medicine, finance sectors and remote work jobs. Technically QEAA's are issued using certified cryptographic keys like QSCDS and signed with qualified certificates. Walt.id supports these via integration with the EBSI framework, allowing the inclusion of X.509 certs [153] and trust metadata in VCs. The verification can follow two paths, either as a DID-based which resolve the issuer's DID and checks the associated keys, or by certificate based where it validate the qualified certificate against the EU trust list.

This dual paths ensures legal certainty and cryptographic assurance. verification is streamlined through checking a digital signature chain making it suitable for automated hiring workflows.

Key Actors in High Trust Issuers Model

The key actors ensures that all issued credentials are anchored in a legally and cryptographically verifiable chain of trust. The use of DIDs and VCs, governed by these actors, enable secure, standards-compliant, and scaleable credential issuance from employment verification across the EU.



Figure 15: A diagram demonstrating the Issuer Trust Model interaction Source: <https://hub.ebsi.eu/get-started/design/trust-chain>

The figure 15 shows the actors and flow for the Issuer trust model as illustrate in EBSI's trust chain where authorisations are expressed as verifiable credentials and on-chain entries that grant specific rights to legal entities. It defines the hierarchy of roles each empowered by explicit credentials in the trust chain.

1. **Root TAO:** Serves as the foundational trust anchor. It is responsible for establishing and publishing governance rules and accrediting subordinate domain-specific TAOs
2. **TAO accreditation:** TAOs issue accreditation VCs to entities e.g., employers or institutions that satisfy eligibility and governance criteria, thereby designating them as Trusted Issuers (TI).

3. **Registries(EBSI Ledger):**These serve as public, on-chain sources of truth where DIDs, schemas, governance policies, and accreditation VC are stored.The registry enables Verifiers to validate the integrity and authenticity of issuers and their credentials.

7.2.2 DID Methods For Legal Entities under the High-level Trust Credentials

This DID method is defined by EBSI specifically for legal entities. Creating a [did:ebsi](#) involves generating a DID document locally and registering it on the EBSI network’s DID Registry, a permissioned blockchain run by authorized EU nodes as explained in section 6.2. Following the onboarding process and accreditation process as earlier explained in this chapter, enhances organizations to undergoes the process to proving it’s identity and obtain permission to write the registry. The DID itself includes a method-specific identifier that is a base58-encoded string guaranteeing uniqueness on the network see Figure 16. Example a company would generate keys and then invoke EBSI’s API to register a DID document, after being authorized through EBSI’s onboarding service. Write access to registry is controlled via EBSI’s authorization service and the DID document’s designated *capabilityInvocation* key. This process adds some overhead to obtain accreditation and perform blockchain registration but it links the DID to an official trust framework, which is valuable for high-assurance credentials in employment verification

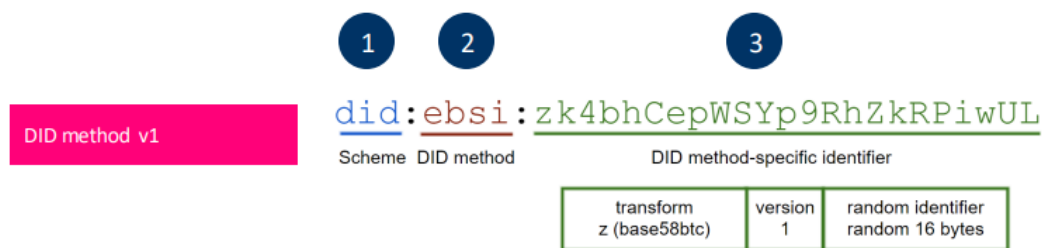


Figure 16: An Example of an `did:ebsi` DID Method v1 Source: [EBSI EXPLAINED](#)

1. DID Document and Key Management

The [did:ebsi](#) DID document can contain public keys and metadata for the issuer. EBSI recommends using W3C *JsonWebKey2020* Verification methods with keys in JWK format and cryptographic algorithms like ES256 as a minimum standard. This aligns with EU eIDAs standards, since ES256 is widely used and supported algorithm in European trust services. Key rotation and updates are supported, the organization can update its DID document in the registry to add or revoke keys over time. All updates or deactivations must go through the DID registry, providing an auditable history of changes. Notably, if an issuer wants an immutable identifier, EBSI allows making the DID non-updatable by clearing its controllers.

2. DID Resolution

Resolving a [did:ebsi](#) involves querying the EBSI Registry typically via an Https API call to retrieve the DID document. The registry serves as the verifiable data registry for those DIDs. Resolution authenticity is ensured by the use of Https and the blockchain’s integrity. The DID document retrieved is the one published by the accredited owner. By default, the latest DID document is returned, but as stated

earlier EBSI's resolver can also fetch the DID document as of a specific timestamp valid-at query for verifying credentials issued in the past. This means that verifiers can check an employment credential and obtain the issuer's public key as it was at issuance time, which is crucial if the issuer has rotated keys since then. The need for online lookup to the EBSI network is a slight dependency however EBSI is a governance-back-end network it is designed for high availability and trust

How Multilevel High Trust Issuers is set up for roles and permissions

With established trust chains ?? centred on multilevel trust framework, intricately linked to EBSI's architecture for accreditation and credential governance proposed structure. As depicted in Figure 17, draws its inspiration from eIDAS regulation's Trusted List and EBSI's trusted registry Framework, effectively establishing a hierarchy of authority among various actors in the ecosystem. For example, a TAO must hold a Verifiable Accreditation to Accreditation issued by RTAO that permits it to accredit other organizations. On the same note, a TI must hold a Verifiable Accreditation to attestations issued by TAO that permits it to issue domain-specific Verifiable credential.

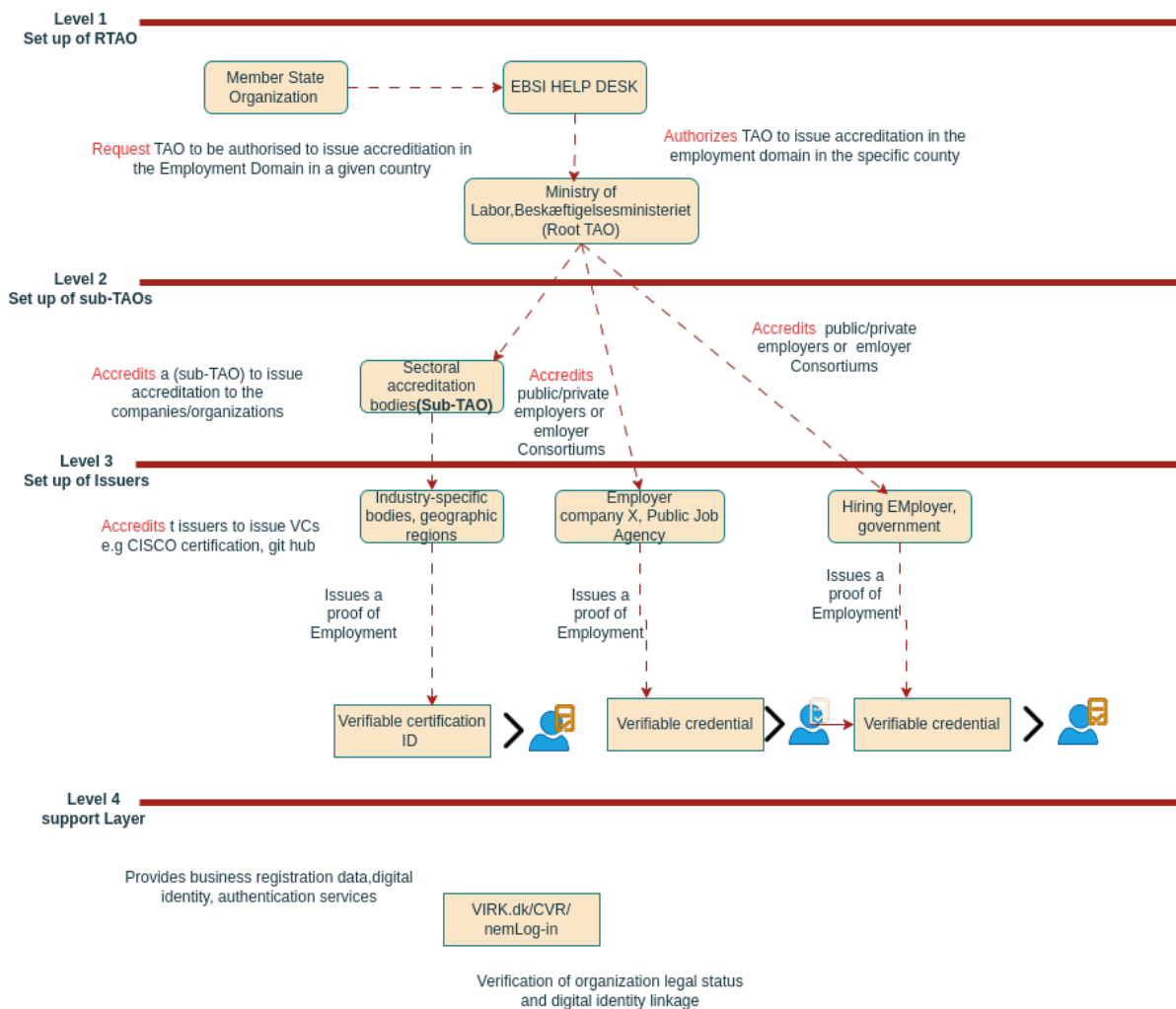


Figure 17: Multilevel Trust set up flow for roles and permissions within the Ecosystem Inspired by EBSI Multilevel guidelines setup

In practice, all these permissions and policies are recorded in the EBSI Trusted Issuers Registry so that a verifier can simply trust the root authority and then cryptographically

validate the entire accreditation chain. Waitid tools support this model directly as their APIs can issue and verify EBSI v3 credentials with the proper trust chain metadata and they provide libraries specifically for EBSI trust registry operations.[17].

1. **Level 1: RTAO Establishment (Ministry or Competent Authority)** At the apex of this trust hierarchy, the establishment of a recognized Trusted Accreditation Organization is initiated by the Member State organization, such as a national labour ministry. This organization embarks on the trust onboarding process by seeking authorization from the EBSI Help Desk to approve a TAO tailored from the employment sector. upon approval, the designated TAO, typically represented by a ministry or national agency, assumes the status of RTAO. This status empowers the RTAO to accredit subordinate entities and formulate governance and policy standards[64]. Furthermore, the RTAO possesses the authority to revoke accreditation from any legal entity involved in the trust chain, a function critical for maintaining the integrity of the accreditation framework.
2. **Level 2: Sub-TAO Accreditation (Accreditation Bodies)** Following the establishment of RTAO, the next tier involves the delegation of authority through the accreditation of subordinate TAOs (Sub-TAOs). These entities, which may include sectoral accreditation bodies like national employment verification boards, are essential in further extending trust within the ecosystem. The RTAO is responsible for accrediting the Sub-TAOs with clearly defined scopes that generally cater to specific industries or geographic regions. By registering these Sub-TAOs within EBSI's Trust registry, the structure enables the propagation of trust to issuing organizations, such as HR departments or employer consortia, thereby reinforcing the ecosystem's credibility[181].
3. **Level 3: Issuer Setup (Employers and Credential Issuers)** The operationalization of this trust framework culminates in the establishment of trusted issuers, comprising employers, public job agencies, and credentialing platforms. Once these issuers receive accreditation from the relevant Sub-TAO, they are authorized to issue Verifiable credentials concerning employment status or qualifications. The scope of these credentials may encompass various types, such as Verifiable Employment Certificates or job title confirmations, all of which are cryptographically signed: such measures ensure compliance with W3C Verifiable credentials Data models and EBSI's DID standards, thus facilitating secure verification processes. Additionally, employers have the capability to manage their digital identifiers and revocation processes efficiently, which is crucial for maintaining trust and ensuring transparency.

This credentials include *termsOfUse* field encoding the trust framework and domain schemas under which the TI may issue credentials. Notably, when TI issues a domain specific VC, that credentials must include an *AttestationPolicy* in *termsOfUse* that links back to the TI's own accreditation and it's root TAO's authorization in the trusted Issuers Registry. Verifiers will check is metadata to ensure the issuer was legitimately empowered and not later revoked to issue that VC.

7.2.3 Low-Trust Credentials and Trusted Issuers

Within the scope of our project, low trust credentials refer to verifiable claims that originate from issuers outside formally governed or legally accredited

frameworks[151]. These include the credentials depicted as Low in our Table 1, these claims are commonly found in traditional CVs but often lacking standardized proof mechanisms.

Unlike high-trust credentials, which rely on inclusion in predefined trust lists such as those mandated by the eIDAS Regulation, low-trust credentials in this system are issued by organizations operating independently through locally hosted and self-managed infrastructures. Trust in these issuers is not derived from formal provenance, and verifier-defined trust evaluation policies[35].

Issuers within this model typically HR departments, line managers, or internal training bodies leverage web-based methods to generate and host DIDs using `did:web` method. Key material used for credential signing is securely stored within their local environment or organizational domain. These identifiers are published and resolved via endpoints accessible over HTTPS, following W3C DID specifications[35].

This decentralized model is inspired by approaches such as European Self-Sovereign Identity Framework (ESSIF), where no central approval is required to become a credential issuer. Any entity can register and publish a DID, allowing them to issue verifiable credentials immediately. Credential exchange occurs in a peer-to-peer manner, with the verifier assuming the responsibility for assessing the legitimacy and relevance of the credential presented[156].

In the context of this system, Credential verifiability is supported through JSON-LD or JWT-based formats, cryptographic signatures, and issuers metadata linked via DID Documents. Trust evaluation is delegated to the verifier, who may use internal policies, schema validation, historical issuer interactions, or cryptographic proofs to assess whether to accept a given credential.

This model supports privacy-preserving verification workflows by enabling holders to disclose only selected attributes from a credential such as employment start date or job title without revealing the full document. This approach aligns with GDPR principles, particularly data minimization and purpose limitation, while maintaining interoperability with our wallet based SSI ecosystems[151].

However, the absence of a centralized trust registry introduces challenges in consistency and assurance. Verifier discretion can lead to fragmented trust evaluation and non-uniform acceptance criteria across organizations. Despite this, the flexibility and minimal onboarding requirements make low-trust credentials particularly suited to decentralized employment ecosystems, especially in context involving SMEs, freelance contracting or informal labour markets.

This project positions low-trust credentialing as the operational core of its issuance model. While high-trust credentials as discussed in 7.2.1 above, are externally referenced and incorporated, the issuance and exchange of low-trust credentials occur natively within the system, enabling rapid deployment, user-controlled credential management, and modular integration with verifiers' existing decision-Making processes.

This model has one type of issuer that is;

EAA (Electronic Attestations of Attributes) Issuers

As defined under eIDAS 2.0, EAAs enable authentication of non-statutory personal attributes, making them ideal for verifying employment related data like job titles, tenure, roles, or training certifications. In our context of use in the employment verification domain, EAA can be issued by both the private and public entities such as employers, universities or professional bodies. They bridge the informational gap left by Personal Identification Data (PID), covering the essential employment

attributes. Despite lacking statutory status, they offer value when issued with cryptographic signatures and integrated into a trust framework like EBSI[24].

EAA onboard by registering an organizational wallet, creating a legal entity DID `did:web`, `did:key` and obtaining accreditation from a trust anchor as highlighted in section 7.4.9 above. Once accredited, their public keys and issuance scopes are listed in the domain specific environment. Walt.id support embedding trust metadata like *credentialSchema*, *termOfUse* within VCs enabling verifiers to validate issuer authorization via the trust framework[118].

Figure 18 shows a high level presentation of these credentials flow

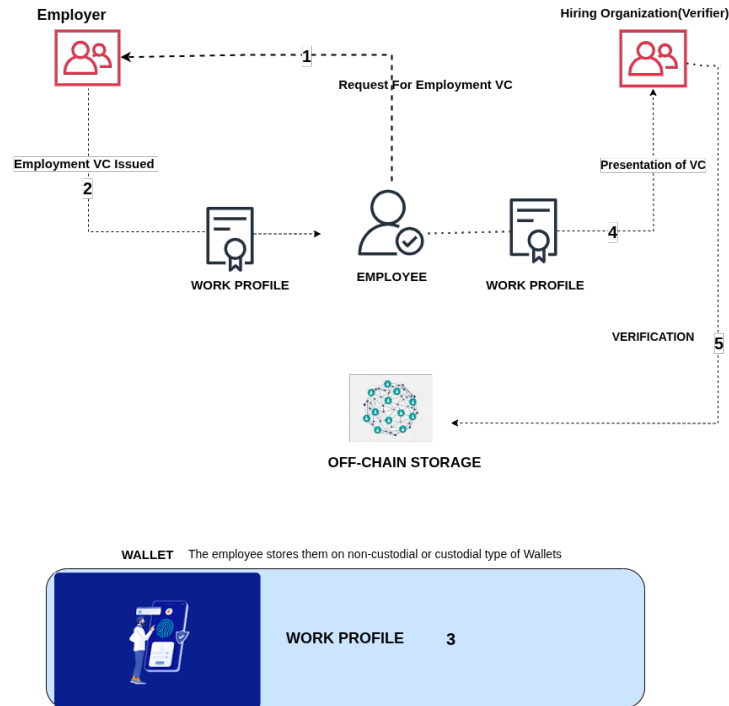


Figure 18: A diagram showing hypothesized Flow of the Employment verifiable credentials in the system

7.3 Towards a Credential Ecosystem for Career Mobility

The analysis presented in this chapter has demonstrated the feasibility of transforming traditional CV elements into modular Verifiable Credentials, supported by both high-trust and low-trust issuance models. Building on this foundation, the notion of a credential ecosystem for career mobility emerges as a strategic trajectory, one which credentials are not confined to isolated hiring events but instead persist and evolve with the individual across roles, industries, jurisdictions and platforms.

In this context, the proposed system contributes towards the development of a decentralized and interoperable credential ecosystem in which individuals can accumulate, curate, and present trusted employment related credentials throughout their professional lifecycle. These credentials issued by diverse actors including employers, universities, licensing bodies, and training organizations can be securely held in digital wallets, managed by the individual, and presented on demand to verifiers without reliance on third-party intermediaries.

Career mobility, particularly in globalised and digital-first labour markets, increasingly requires mechanisms that enable portable, trustworthy, and verifiable

professional records. The current model of static document-based CVs lack the capability to support such fluidity, especial in cross-boarder hiring scenarios or freelance and gig economy contexts. By contrast, Verifiable credentials offer cryptographic proof, issuer traceability, and privacy-preserving sharing mechanisms key attributes for enabling mobility without compromising trust or compliance.

This ecosystem approach is further reinforced by the layered trust model adopted in the system architecture. We highlight the use of high-trust credentials from Walt.id framework demo accredited issuer domain, and how they provides strong foundation layer to verified identity and qualifications, while the emphases is no low-trust credentials captured in domain-specific experience and competencies. When combined, these layers produce a rich, verifiable identity footprint that can be selectively disclosed depending on the verifier's assurance requirements and contextual needs.

Moreover, the system's compatibility with existing European frameworks such as EBSI and eIDAS ensures forward compatibility with evolving trust and interoperability standards. This opens pathways for inclusion in larger trust ecosystems, including public service hiring, regulated industries, and transnational credential registries.

The move toward a credential ecosystem for career mobility therefore represents more than a technical enhancement, it reflects a shift in how professional identity is managed, verified, and trusted in digital society. The project's contribution lies in establishing a scalable architecture, rooted in Self-Sovereign Identity (SSI) and Verifiable Credentials, that not only enhances hiring processes but also lays the groundwork for a truly portable, lifelong career identity.

7.4 Technical Considerations For The Design of the Employment Verification System

In these section, we outline the technical parameters guiding into the design of the employment verification system, with particular focus on low-trust credential issuance. It examines how components discussed in 5, DIDs, digital wallets, credential schemas, signature mechanisms, and web-based issuer infrastructure are orchestrated to support scalable, privacy-preserving, and verifier driven trust evaluation. This discussion is grounded in W3C and SSI standards and considers practical deployment within a self-managed, domain-specific environment. These considerations inform the system's architectural model presented in the subsequent chapter.

7.4.1 Credential Model and Data Elements

As part of our project's approach to decentralised employment verification, a well-defined credential is required to represent selected CVs claims as verifiable, structured document. In this analysis, we outline what role the credential model will serve, what is expected to include, and what it intentionally excludes based on the scope and trust assumptions established earlier.

The credential model will serve as a structured representation of all employment information sythesis, intended to be issued by employers acting as low-trust level issuers and held by employees within their personal digital wallets. It forms the basis for converting previously informal or unverifiable data such as job titles, durations and responsibilities into digitally signed credentials that can be independently verifies. The model applies specifically to;

- Employment data derived from internal HR systems or records

- Low -assurance attributes such as department, role descriptions
- Data elements that do not require state recognition or legal endorsement to be accepted.

The project will not include high-trust data elements such as academic degrees, legal identity claims, or professional licenses that fall under the domain of regulated or qualified trust service providers. Instead, those are assumed to be issued within external ecosystems such as EBSI, may be referenced as supporting credentials in a composite verifiable agent model.

The data elements purposefully selected to reflect the core informational needs of employers, recruitment platforms, and regulatory bodies involved in job market transactions. They include the following **claim-specific attributes**:

- *job Title*: Formal designation held by the employee;
- *employment Type*: Nature of the contract (e.g., full-time, part-time, freelance);
- *Department or Unit*: identifies the role match and functional alignments;
- *start Date, end Date*: Duration of the employment relationship;
- *role Description*: Description of tasks or competencies demonstrated;
- *optional metadata*: Primary location, region of employment or employment ID;
- *supervisor* (optional): Reference to a supervisory DID for relational proof.
- *Credential Status* active or revoked

These fields will be grouped under the *credentialSubject* in accordance with W3C VCs standards. The identifiers used, DID of the holder, the DID of the issuer and the proof mechanism are aligned with the decentralized identity frameworks. This model supports the goals of the system by enabling, partial automation of verification, without the email or phone calls for HR. Fine-grained attribute disclosure by sharing only what's needed, and lifecycle management of the credentials,

In the design chapter, this model will be extended into concrete credential schemas and workflows. For now the analysis confirms that the credential model will focus on verifiable, employer-attested claims, excludes high-trust institutional data, and is scoped to support low-trust issuers operating under web-based DID methods. The schema is modelled in JSON-LD for semantic interoperability, with optional support for SD-JWT encoding to enable *selective disclosure* a privacy-enhancing feature that allows the holder to reveal only the attributes relevant to a given verification context.

7.4.2 DID Methods For Verification in the Decentralized Employment System

In our system, we identified a core requirement or establishing trustworthy links between the credential, the organization issuing it, and the individual presenting it. This has led us to examine the role of DIDs, more specifically, the distinction between DID Methods used for the employees or job seekers in the system, and the DID for the employer who are the organizations who issued them.

our system depends on this differentiation not for the purpose of managing access or delegating roles, but rather to ensure that the employment credentials can be cryptographically bound to both the issuer and the holder in a way that strengthens

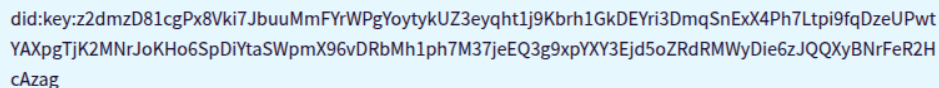
trust, accountability, and verifiability. This is particularly important given the nature of employment verification, where the claim being made ".i.e., Sofia worked at Y during Z period" must be demonstrably linked to both parties involved.

DID Methods For The Job Applicants/Employees (Natural Persons)

Within our system, natural persons, primarily employees who are the holders and presenters of employment credentials require a form of identification that is both verifiable and privacy-preserving. As part of our analysis, we examined the use of lightweight and self-managed DID methods for this purpose, with a focus on `did:key` and `did:jwk`.

These methods are selected based on several key factors aligned with our system's core values; decentralized, minimal reliance on centralized infrastructure, and strong user control. Both `did:key` and `did:jwk` support these requirements by allowing individuals to generate DIDs locally through their digital wallets, without needing to register on a distributed ledger or maintain any form of public resolvability[131].

For example if a user generates an Ed25519 or ECDSA key, the `did:key` might look like in the Figure 19 where the string after `did:key` is a multi-base representation of the public key. The feasibility of creation is extremely high as any modern device can create a secure random key in milliseconds. EBSI has also adopted `did:key` as the required method for Natural persons precisely because it avoids putting personal identifiers on a permanent ledger and thus better protects privacy. Thus, in our system, a user would typically have their identity wallet in walt.id's wallet, generate a new `did:key` for them when they onboard hence, becoming the decentralized identifier for receiving credentials[48]. No central authority is involved however in an ecosystem context, the user might need to prove their real-world identity at some point. For instance, to the issuer when obtaining a credential. That proof could be done out-of-band by just showing the ID document or via another credential, but most importantly the `did:key` generation itself is under the user's control[34],[41].



```
did:key:z2dmzD81cgPx8Vki7JbuuMmFYrWPgYoytykUZ3eyqht1j9Kbrh1GkDEYri3DmqSnExX4Ph7Ltpi9fqDzeUPwtYAXpgTjK2MNRJoKH06SpDiYtaSWpmX96vDRbMh1ph7M37jeEQ3g9xpYXY3Ejd5oZRdRMWYDie6zJQQXyBNrFeR2HcAzag
```

Figure 19: an Example of DID method for Natural Personal

7.4.3 DID Methods for Employers and Organizations (Legal Entities)

As part of the answer to our research question on how trust in the issuer can be propagated, legal entities issuing employment credentials can use two DID methods namely; `did:key`, and `did:web`. Both methods let organizations serve as trusted credential issuers, but they differ in how DIDs are created, resolved, delegated and trusted.

Unlike the formal public infrastructure such as EBSI network, which uses `did:ebis` to represent organizations within a regulated, permissioned blockchain, our project applies a more flexible and lightweight model. We rely on `did:key` to represent legal entities issuing credential in our controlled, sandboxed environment.

The use of `did:key` in our context stems from the practical requirements of the system; Self-contained Trust, they allow an issuer to generate a decentralized identifier directly from a cryptographic key pair, without requiring registration on a blockchain or third-party registry. This fits well within our deployment model, where trust is

established within the boundaries of a known consortium or internal network like Hyperledger Besu using PoA consensus, Simple onboarding, unlike the EBSI's did:ebsi which mandates a rigorous onboarding and accreditation process through its authorization service, did:key can be immediately generated and used by the organizations' credential issuing service. This reduces administrative overhead and accelerates setup during testing and early-stage rollouts, and lastly, local verifiability, even though did:key lacks public resolvability, in our system all participants issuers, verifiers and holders interact within a common trust domain where the DID Documents and corresponding public keys are directly exchanged or cached. This circumvents the need for global resolution infrastructure and supports a controlled trust propagation model.

While this approach does not embed the issuer into a public or government-backed trust framework as did:ebsi would, it supports a privacy-respecting and technically interoperable issuance process. Moreover, in our case, the employer's DID is still used to sign verifiable credentials, and the verifier checks the signature against the known DID Document ensuring cryptographic authenticity even without blockchain anchoring.

This decision aligns with the system's design principle of being modular and flexible while preserving core SSI principles. It also reflects the realities of early-stage or non-production environments where formal accreditation (as with EBSI) may be infeasible or unnecessary.

On the other hand, the *did:web* method uses the existing web infrastructure as its base. A did:web identifier is essentially tied to an internet domain name, under which the DID Document is hosted. To create a did:web, a legal entity needs to own a DNS domain or subdomain and publish a DID document at a standard location. An example here would be <https://yourdomain.com/.well-known/did.json> or a path under the domain. The DID itself is formatted as *did:web:yourdomain* with path segments for subdirectories if needed. No permission from a central authority is required beyond the normal domain registration as an organization can create a did:web by controlling a domain and hosting the file making them very accessible and quick to create.

An instance of application would be, a company that wants to start issuing employment VCs could generate a DID document containing the company's public key and other metadata and uploads it to their portal. The process utilizes the existing IT skills like editing a JSON file on a web server rather than blockchain transactions. However, because there's no ledger enforcement, uniqueness and control rely on the DNS. Feasibly when implemented, any employer with an official portal can set up a did:web within minutes which lowers the barrier to adoption for those not yet integrated with EBSI.

Resolving the did:web involves fetching the DID document over HTTPS. Trust is anchored in the web PKI, if the server presents a valid TLS certificate for the domain, the verifier trusts the DID document thus enabling credential verification through standard internet protocols without needing ledger interaction. This means that that verification of an issuer's signature with did:web involves an online HTTP lookup, for instance, a verifier receiving a credential issued by *did:web:hr.company.com* would perform an Https GET on hr.company.com to retrieve the public key needed to verify the credential.

They support basic key rotation and delegation via its DID document as organizations can manage signing keys or delegate authority to subunits as mentioned in HR department above by publishing DIDs on subdomains. Updates are then managed by simply editing the JSON document similar to managing DNS or SSL through without cryptographic audit trails in did:ebsi. This solution offers an easy onboarding path for

small or unregistered employers. it's ideal for rapid deployment or non-critical use cases.

7.4.4 Credential Status and Lifecycle Management)

Credential status referring to the current validity state of a credential, is a crucial element in maintaining trust within the decentralized employment verification system. Trust does not only rely solely on the issuance or presentation of the credential, but also the ability to determine whether it remains valid at the time of verification. This requires a robust lifecycle management approach, encompassing issuance, validity, duration, revocation and status tracking.

Natural Person Credential Status and Lifecycle

In our system's context, workers or job candidates receive VCs such as proof of employment, role attestations, or contact duration statements from authorized legal entities. These credentials must reflect facts that are subject to change. For example, when an employee resigns, is terminated, or undergoes a role change, previously issued credentials may no longer be accurate and must be either revoked or updated to prevent misuse.

A concrete example is a VC that asserts *"Sofia is employed as an Engineer at company X."* If Alice leaves the company, this credential must be flagged as revoked to ensure it is no longer valid. Such real-time responsiveness protects verifiers from relying on outdated or inaccurate information, and uploads the credibility of the broader trust ecosystem.

However, because these credentials pertain to natural persons, they fall under GDPR protections, meaning their status data can not be stored directly on-chain. Instead, privacy preserving status management techniques must be applied such as off-chain status lists, encrypted revocation registries, or ephemeral credential expiration mechanisms to allow verifiers to assess status without exposing personal information.

The EBSI trust architecture and by extension the walt.id framework, provides an interoperable mechanism for communicating the revocation or suspension status of issued credentials to verifiers, without compromising the holder's privacy or requiring direct online verification from the issuers

Legal Entities Credential Status and Lifecycle

Revocation and accreditation status management of VCs issued to employers, agencies, or other certifying bodies are critical components in a decentralized employment verification system. Unlike credentials tied to individuals, issuer credentials are not subject to GDPR and can be publicly managed via registries like EBSI's Trusted Issuers Registry and local domain directories. This allows verifiers to check whether an organization is currently authorized to issue employment-related credentials. Maintaining accreditation status information also ensures that legal entity meets the criteria set by a trust framework or regulatory body.

To support this, proposal for two strategies for verifiable Accreditation issuers to store and manage the status of the credentials they issue, enabling revocation, suspension, or updates when an entity loses its eligibility. This is particularly important in cases of organizational changes, non-compliance, or license expiration. Technically, revocation and accreditation status can be implemented using the mechanisms like StatusList2021 or policy-based registries, enabling real-time validation and trust enforcement during VC verification. Integrating these controls

reinforces the reliability, interoperability, and compliance of the employment verification system at scale. The figure 27 below illustrates the process;

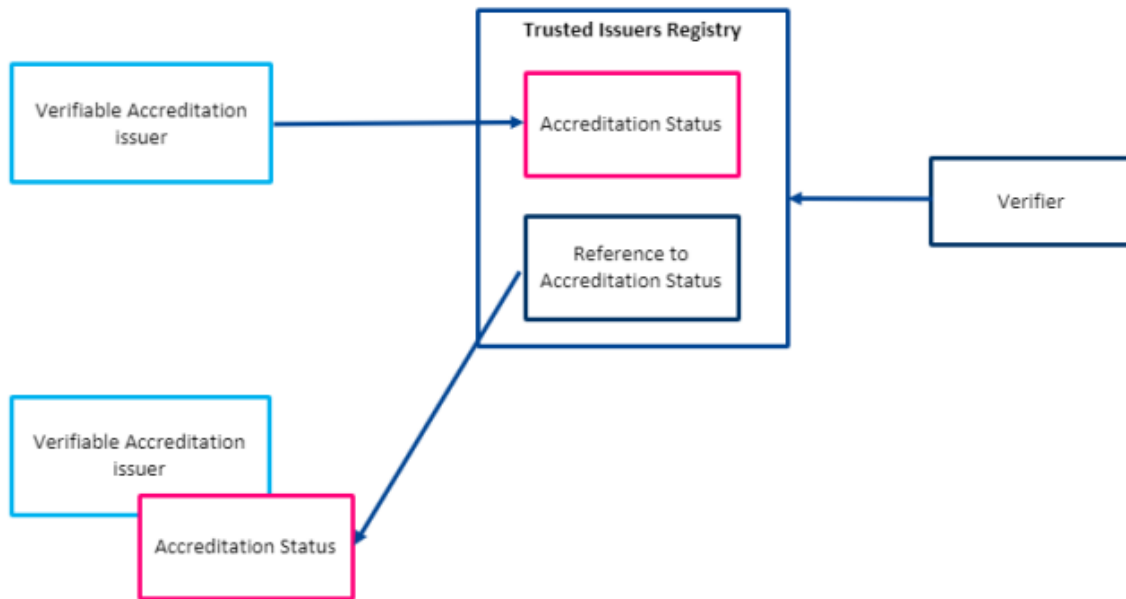


Figure 20: Accreditation status information storage for verifiable Accreditation Issuers

7.4.5 Verifiable Attestation Management Strategies for Employees/Job Seekers

As part of the solution to the research question 1.4, managing the status of VCs issued to natural persons is essential to ensure the ongoing validity of employment claims. Since these VCs often change as described in above due to resignation, termination or contract expiration. Our solution supports mechanisms to handle their revocation, suspension.

The diagram 21 illustrates the strategies interactions between holders, verifiers and issuers of different VCs with different strategies.

1. Reissuing Short-Lived VCs On-Demand

In this strategy, short-lived employment credentials like contract confirmation or temporary project roles are not revoked but instead reissued whenever needed. The holder requests a new VC for each use, eliminating the need for revocation infrastructure.

The role in our system would be;

- Suitable for temporary employment scenarios or freelance verification, remote works.
- Simplifies verification as verifiers only check the expiration timestamp.
- Ensures that only up-to-date employment are shared.

However the trade-off with this strategy is that it requires real-time VC issuance, meaning that both the holder and issuer must be online thus the issuers may learn when and how often VCs are requested and that raises privacy concerns.

2. Direct Status Check from Trusted Issuer

This strategy is best suited for low-trust long-lived credentials, where revocation or suspension is managed by the issuer, and verifiers fetch status directly from the issuer's endpoint.

The role in our system would be;

- Ideal for full-time employment VCs or position attestations.
- Ensures real-time trust validation even if the holder is offline.
- Useful when organizations already maintain their own revocation APIs.

With this strategy issuers may learn who is verifying which credentials, potentially compromising privacy and the verification windows are harder to restrict from the holder's side.

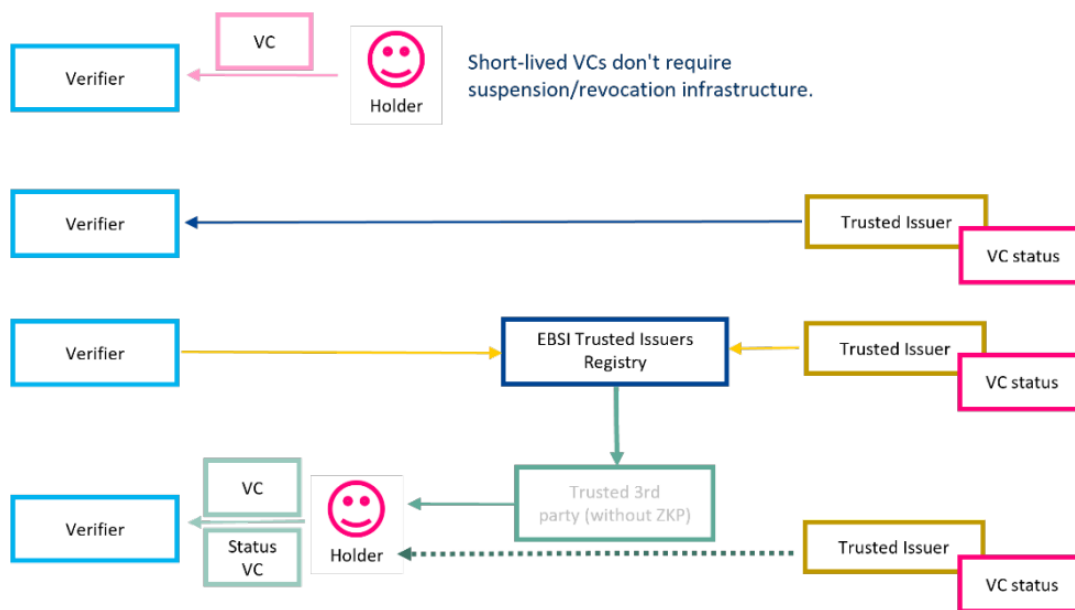


Figure 21: Verifiable Attestations Management Strategies for Natural Persons

3. Status Check via EBSI Mediation

In this strategy, issuers push status data to EBSI, allowing verifiers to retrieve revocation or suspension information without directly contacting the issuer.

In our systems, this balances trust and privacy as it is suitable for high-trust credentials tied to regulated roles such as medical, legal or compliance-critical jobs as we have described in 3.3 section. This strategy is important as it enables status verification even when the holder's wallet is offline. It also reduces network load on the issuer while supporting GDPR compliance.

It heavily depends on status list formats, holders may not control how long verifiers can access the data.

4. Status VC Held by the Individual

In this strategy the holder is issued a separate VC that encapsulates the status of an existing credential. This may be signed by the issuer or third-party authority i.e. Azure, Keycloak etc..

The role in our system would be;

- Empowers holders with offline verifiability of employment VC status
- Enhances user control and portability, aligning with SSI principles

The disadvantage of this strategy would be that it requires issuance and management of an additional VC, increasing system complexity, and it also relies on verifiers trusting the third-party if not the original issuer

7.4.6 Verifiable Accreditation Management Strategies for Legal Entities

1. Accreditation information stored in DLT Trusted Issuers Registry

As discussed with our High-trust credentials, this involves storing the verifiable status information directly in the Trusted issuers Registry, which leverages DLT to ensure secure and tamper-evident management of issuers metadata. In this model, the verifier queries the registry to retrieve the current status of an issuing legal entity. The registry acts as a trust intermediary, removing the operational burden from issuer to host or maintain the status themselves.

2. Accreditation information hosted by the issuer and obtained via DLT Trusted Issuers Registry

This strategy used for our low-trust credentials delegates the responsibility of hosting accreditation status information to the issuer, while still making it accessible via the Listed Trusted Issuers Registry. This allows the issuers to retain control over their own accreditation data while benefiting from the registry's integrity guarantees and standardized access interface. This is especially suited for organizations that already maintain internal systems for managing accreditation and seek to integrate them with decentralized trust infrastructure.

7.4.7 Accreditation process for high-trust credentials

Accreditation refers to the formal recognition by a governing or trusted authority that an Entity typically an issuer is authorized to issue specific digital credentials or perform designated roles within the trust framework. In decentralized identity ecosystems, accreditation is implemented through VCs that delegate authority. A verifiable Accreditation, for instance, is defined as a signed credential that delegates authority from one entity to another, specifying the types of credentials they are permitted to issue[98]. In practice, Accreditation establishes a trust anchor in the ecosystem. A high level authority as highlighted 7.2.2 anchors a hierarchical trust model all through to the issuers, thus accreditation is what binds issuers to governance. An issuer's Verifiable Credential e.g., Diploma references to its accreditation allowing verifiers to confirm that the issuer is trusted as it's accredited by a TAO as shown in Figure 22 Below.

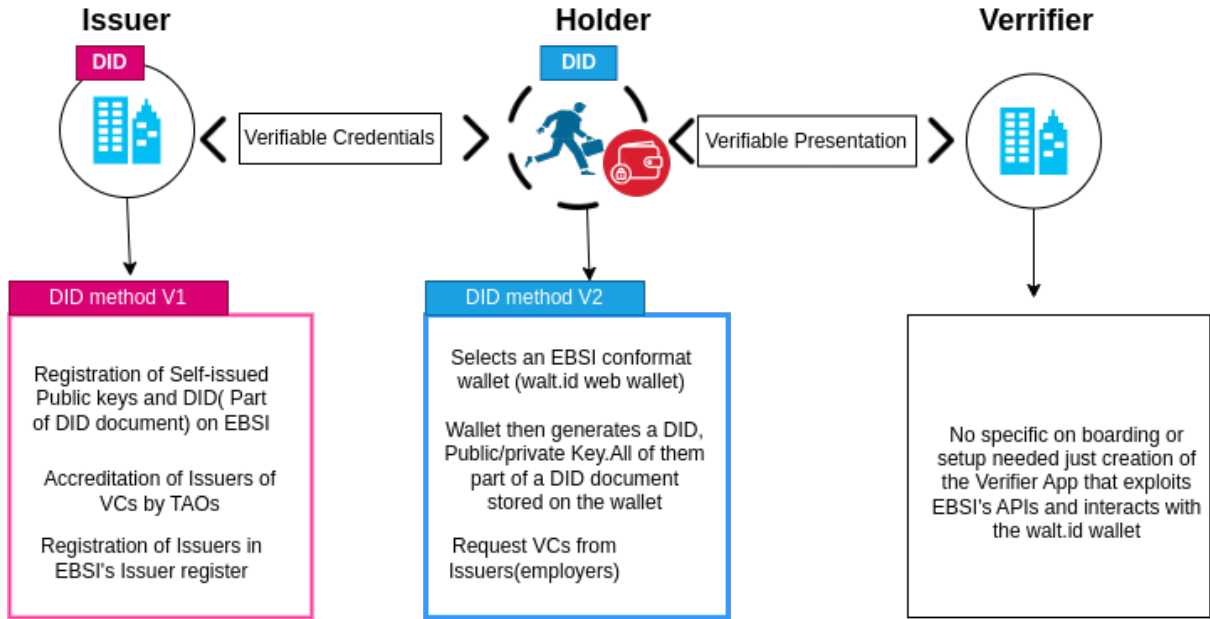


Figure 22: Example of the Accreditation process of the Issuer onboarding

In essence, accreditation in DID systems ensures that every credential is sourced from a legitimate, pre-approved entity within a defined domain, thereby fostering reliability and interoperability within the digital trust ecosystem[92]. The significance of accreditation lies in its ability to establish decentralized trust, substituting ad-hoc or manual verification processes with a cryptographically anchored trust chain: Each accreditation VC is digitized and stored in Trust registry or trust lists, and these registration is anchored in a distributed Ledger, offering a tamper-evident record of who is authorized to issue what type of credentials.

Accreditation emphasizes the interconnection of technical mechanisms like digital signatures, DIDs and registries with legal authority defined in the governance frameworks. This allows verifiers to automatically validate credentials across varying organizational or national boundaries. Ultimately, accreditation ties together the technical and governance aspects necessary for establishing digital trust, which is crucial for ensuring the efficiency of decentralized identity solutions

Many DID/VC platforms integrate support for these trust construction. Walt.id SSI stack includes modules for EBSI. Its documentation notes that entities must register and get accreditation before issuing in an EBSI trust chain, and its issuance API includes fields for accreditation. When issuing an EBSI-compliant credential, walt.id's API expects the *issuerDid* and *issuerkey* to correspond to DID/key registered on EBSI, and it uses a *termsOfUse* attribute to encode the value of the accreditation. In effect the tool chain embeds accreditation references into the credential payload. Case studies have shown organizations issuing accreditation certificates via walt.id for instance the European Quality assurance Register used walt.id to issue EBSI-compliant university accreditations as VCs based on its DEQAR datasets[44]. Thus modern DID framework make it easy and straightforward to handle accreditation cryptographically as signed credentials and to interact with trusted registries for recording and verification.

7.4.8 Key Management and Security

Since did:key DIDs are derived from the key generation, key management for the user is critical. The user's private key must be stored securely, because losing the private key

means losing control over the DID and any credential tied to it. Walt.id's web wallet handles key storage, typically by encrypting keys on device or using secure enclaves. EBSI's guidance emphasizes compliance with eIDAS requirements for credential security like keys should ideally be generated and stored in secure hardware or at least with strong protection[41].

If higher assurance is needed let's say like for binding the DID to an organization's ID or a high value credential, the wallet might use a qualified signature creation Device or hardware security module to manage the keys. It is highlighted that did:key management should be similar to managing personal cryptographic token or password manager, where, users need good UX to backup and secure their keys. The did:key method however does not support key rotation per Se as the DID is the key. If a user needs to rotate their key for any reason like compromise or upgrade, that may result to a new did:key[34].

For our design, this means that if an employee loses their wallet or needs a new key, they might need to get their credentials reissued to a new DID, or use some recovery mechanisms outside the DID which are not covered in our project as this is out of scope simply because this is more of an operational consideration than a fundamental roadblock. In practice, because issuing a new credential is easier than, say, reissuing a passport, this limitation is manageable. The system can encourage individuals to maintain safe backups like a seed phrase or cloud backup encrypted for their DID keys. Walt.id's wallet kit supports exporting/importing keys and could be integrated with custodial solutions if necessary for recovery.

7.4.9 Sequence of High-trust Establishment and Credential Flow

The process of establishing trust and managing credential flows in the decentralised system involves several key steps. Initially the Root Trusted Authority Operator (TAO) publishes its DID and governance framework on the EBSI ledger, thereby creating a transparent and immutable trust anchor that serves as the fundamental point of verification[159]. This publication ensures that all subsequent interactions rely on a publicly auditable record, reinforcing both the transparency and integrity intrinsic to blockchain-based SSI systems.

Following the initial registration, Root TAO proceeds with the accreditation of domain-specific TAOs. In this stage, the Root TAO issues a verifiable credential to entities such as national labor authorities, thereby attesting to their accreditation status. This accreditation creates a hierarchical trust chain that's critical for maintaining the integrity of digital identity ecosystems, ensuring that only vetted and authorized entities participate in the credentialing process.

Subsequently, the accreditation domain-specific TAO endorses the process of issuer accreditation by awarding an Accreditation VC to employers or institutions. Once issued, these organizations must register as Trusted Issuers in the EBSI registry. This step mirrors established practices in decentralized identity management, where the verification of issuer legitimacy is essential to secure the end-to-end credibility of digital credentials.

Once issuer accreditation has been completed, the actual process of credential issuance takes place. Here, a recognized issuer creates and digitally signs a VC, for example, one that evidences proof of employment, role affiliation, or position tenure, thereby providing the credential holder, typically an employee, with a verifiable record of their affiliation and achievements. This signed credential serves as an immutable attestation, staking its legitimacy on cryptographic assurances and the underlying trust framework.

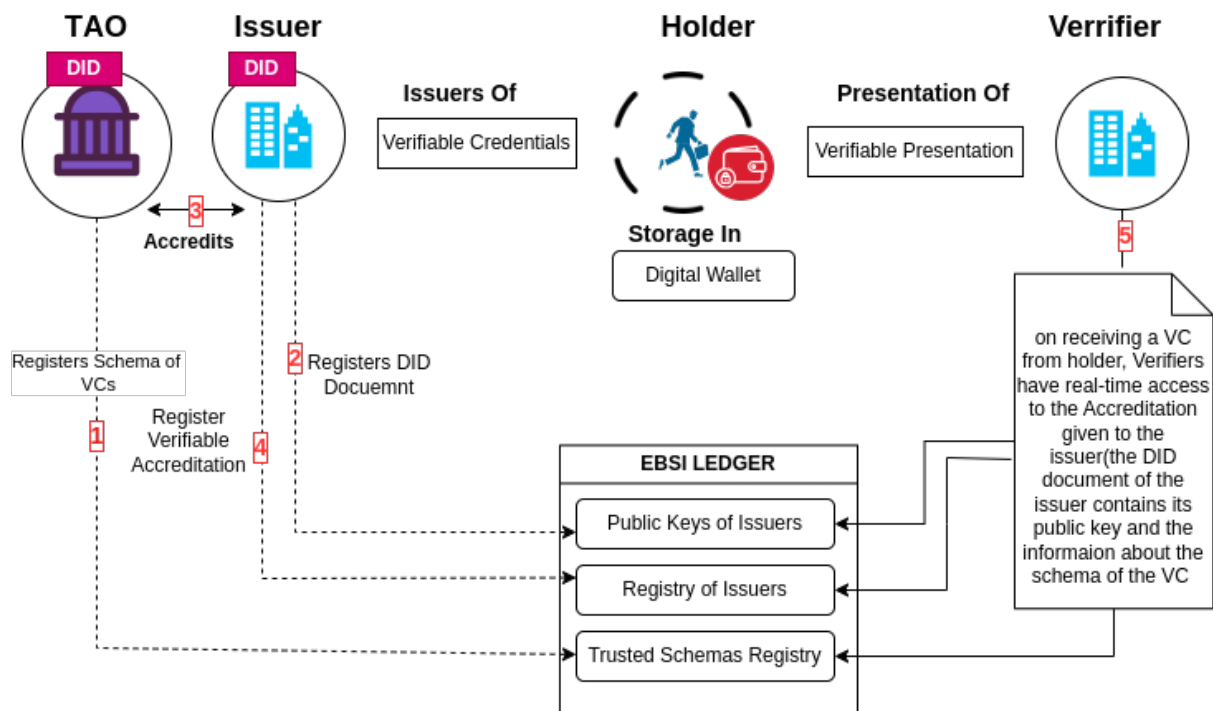


Figure 23: How to establish Trust between the Issuers and Verifiers [Diagram Inspired by EBSI](#)

The final phase involves the presentation and verification of credentials. In this phase, the credential holder selectively discloses specific elements of the VC to a verifier based on the requirements of the verification process. The verifier then undertakes several key verification steps, including resolving the issuer's DID from EBSI ledger, checking the accreditation status through the trust registry, validating digital signatures against established governance frameworks, and querying a credential status list to ensure that the credential has not been revoked. This comprehensive verification mechanism upholds the security and non-repudiation of the credentials within the decentralized framework while conforming to privacy-preserving principles.

This structured sequence from root registration to the final presentation and verification embodies a robust approach to trust establishment and credential flow management within decentralized systems. The approach integrates multiple layers of verification and accreditation processes that collectively ensure the authenticity, integrity and trustworthiness of issued credentials, thereby supporting a secure and resilient digital identity ecosystem as shown in Figure 23 above.

7.4.10 Revocation Registry

The W3C Verifiable Credentials Data Model 2.0 defines a standard way to represent credential status, ensuring interoperability across systems. In this model, a credential can include a *credentialStatus* field that points to status information maintained by the Issuer. The goal here is to let any verifier universally check if a credential has been revoked or suspended, according to an agreed format. One widely adopted method is the Status List 2021 specification. Status List 2021 provides a standardized, privacy-preserving way to publish the revocation status of many credentials in a single data structure.

- **Status List 2021:**

Uses a bitstring to represent the status of credentials. Each issued credential is assigned an index in this bitstring, the bit at that position indicates the

credential's status, commonly 0 for valid and 1 for revoked. The entire bitstring is highly compressible, and the composed bitstrings are then stored in a Status List credential, which is itself a verifiable credential signed by the issuer. This status List credential contains an identifier, a type, e.g. StatusList2021Credential, the Issuer's DID, a timestamp, and a credentialSubject that includes the encodedList and a statusPurpose field indicating what kind of status is being tracked.

```

1  {
2    "@context": [
3      "https://www.w3.org/2018/credentials/v1",
4      "https://w3id.org/vc/status-list/2021/v1"
5    ],
6    "id": "https://issuer.walt.id/credentials/status/3",
7    "type": [
8      "VerifiableCredential",
9      "StatusList2021Credential"
10   ],
11   "issuer": "did:web: issuer.walt.id",
12   "issuanceDate": "2021-04-05T14:27:40Z",
13   "credentialStatus": {
14     "id": "https://example.com/credentials/status/3#94567"
15     "type": "StatusList2021Entry",
16     "statusPurpose": "revocation",
17     "statusListIndex": "94567",
18     "statusListCredential": "https://example.com/credentials/status/3"
19   },
20
21   "credentialSubject": {
22     "id": "https://issuer.walt.id/status/3#list",
23     "type": "StatusList2021",
24     "statusPurpose": "revocation",
25     "encodedList": "H4sIAAAAAAAAAA-3
26                     BMQEAAADCoPVPbQwfoAAAAAAAAAAAAAAAAAIC3AYbSVKsAQAAA"
27   },
28   "proof": {
29     "type": "Ed25519Signature2018",
30     "created": "2021-04-05T14:27:40Z",
31     "proofPurpose": "assertionMethod",
32     "verificationMethod": "did:web:issuer.walt.id#keys-1",
33     "jws": "eyJJ...<signature>...zIg"
34   }
35 }

```

Listing 1: StatusList2021 VC Revocation Example

This means the credential is the 3rd entry in the issuer's revocation status list. The verifier will retrieve the status Status List VC from the given URL as depicted in Diagram 1 above, verify its signature, ensuring it's from the trusted issuer, decompress the encodedList and check the bit at position 94567.

Beyond Status List 2021, there are other revocations to consider, each with its trade-off and the design and accommodate of multiple;

- **Certificate Revocation Lists:**

CRL can serve as an extended mechanism for managing the status of verifiable credentials issued by legal entities such as employers, staff agencies etc. Unlike simple status list that indicates whether a credential is valid or revoked, a CRL provides richer metadata, such as the revocation date, reason for revocation and other context-specific details. For instance, an industry accreditation authority could use a CRL to track the status of employers' accreditations. if an

organization loses its right to issue employment credentials, the CRL could indicate when the accreditation was revoked and why, like due to non-compliance, regulatory breach or voluntary withdrawal. This added granularity enhances the transparency, auditability, and risk management capabilities of our verification ecosystem, especially in use cases involving sensitive or regulated employment roles.

- **On-Chain Credential revocation registry:**

In certain contexts e.g legal entity or accreditation credentials, EBSI permits credential status to be stored on-chain using DLT-based registries, while off-chain methods are preferred for personal data due to GDPR, on-chain revocation is viable for non-PII-based credentials

- **Simple Revocation Registries:**

These involves DID-linked endpoints that return Boolean Values or timestamped status indicators. Although simpler, this approach is less scalable and not privacy-optional for larger-scale deployments like employment verification ecosystems. Thus we do not plan to implement this model

Ultimately, we will likely implement off-chain status list conforming to W3C StatusList2021 standard, given its efficiency and alignment with VC Data Model 2.0. This means that every credential we issuer will reference a status list entry. The issuer must maintain and publish the status list, and the verifier must check it during verification.

7.4.11 Types of Revocation in the Employment verification

- **Immediate Revocation:** Encompasses the capability to invalidate a credential on-demand, promptly rendering it invalid when circumstances necessitate such an action. In the proposed architecture, this is operationalized through toggling a status bit associated with the credential index on the Status list from "Valid (0)" to "Revoked (1)". The technical execution of this strategy is straight forward, the issuer updates the status list by modifying the bitstring and subsequently republishes or re-signs the Status List Verifiable Credential. As a result, verifiers who retrieve the updated list can ascertain the credential's revoked status.

A paramount challenge associated with immediate revocation pertains to the propagation of changes and ensuring timeliness in the update dissemination to verifiers. With strategies such as online fetch or blockchain event notifications, it is possible to achieve near-real-time updates. The EBSI suggests that status lists should be refreshed either with each status change or on a periodic basis, potentially allowing for grace periods between updates. For high-stakes scenarios such as an employee's termination for misconduct, immediate updates are imperative to mitigate the potential for credential misuse.

- **Expiry (Time-Limited Credentials):** Another strategy involves the issuance of credentials tethered to an expiration date. For instance, an employment VC could be pre-set to expire upon reaching the contract end date. In this framework, post-expiration, the obligation for an explicit revocation action diminished, as verifiers can independently assess the credential's expiration date and ascertain its invalidity thereafter. This approach is characterized by its simplicity it operates effectively when the credential's validity period is predictable or when short-lived credentials align with operational needs.

- **Suspension (Temporary Invalidation):** Suspensions refer to the ability to categorize a credential as inactive without enacting a total revocation. Within employment contexts, this is particularly relevant for scenarios such as an employee being on maternity leave or undergoing a performance review, where their credential may need to be suspended temporarily but later reactivated. The technical implementation of this can be achieved through defining distinct statuses within the status list.

An issuer may maintain two separate bitstrings, one dedicated to permanent revocation and another to temporary suspension, thus enabling the credential's *statusField* to include dual entries, both revocation and suspension. For instance, an employment VC could simultaneously appear as revoked with the revocation bit of 1 and suspended with a suspension bit of 1, with the revocation bit remaining at 0. Verification protocols would then necessitate the exploration of both lists, if a credential's status appears invalidated in either category, the verifier would reject it. The walt.id Framework exemplifies this method by facilitating multiple status entries on a single credential, enabling an agile manoeuvring through various states of validity without permanently severing the credential's operational capacity.

7.5 Regulations and Legals Consideration Analysis

The regulatory feasibility of our systems is reinforced by its alignment with privacy-by-design, data minimization and storage limitation principles as required by the GDPR. One of the central challenges in designing privacy-respecting systems is recognizing that privacy expectations vary across jurisdiction, use cases and workflows.

7.5.1 Consent Management

In our proposed system consent is interactively granted by the holder through their digital wallet. When a verifier requests credentials typically via an OpenID4VP flow, where the wallet authenticates the user, lists matching credentials, and prompts the user to approve sharing. To comply with GDPR Article 7(1), this consent must be recorded, often as a cryptographic consent receipt detailing the parties involved, data shared, and the purpose, following ISO 29184 guidance.

The Consent should also be able to be withdrawn at any time, as mandated by GDPR article 7(3), through refusal to share or deletion of the credential. Technically, this triggers updates such as marking the credential as revoked as described under 7.4.4 above, ensuring it can no longer be used.

The walt.id framework provides the technical infrastructure for this consent-based interaction model, including support for OpenID4VC, credential status tracking, and DID document resolution, ensuring compliance with both technical interoperability and regulatory safeguards.

7.5.2 User control via digital wallets

A core tenet of SSI and the W3C VCs architectures is the user-centric data control through the use of digital wallets. These wallets serve as secure agents for managing DIDs, storing VCs and facilitating consent-based credential presentation. Within the scope of this employment verification system, digital wallets are instrumental in

establishing decentralized trust, enabling privacy-preserving interactions, and ensuring alignment with data protection regulations

From the issuer or verifier perspective, legal entities may operate digital wallets to manage their organizational-level identifiers and credentials. These institution wallets enable organizations to:

- Issue VCs to individuals, such as employment attestations, job role confirmations, or contract durations statements
- receive and verify credentials during onboarding, auditing, or third-party intergradation processes.
- Establish trusted relationships with registries and accreditation bodies by participating in DID-authenticated onboarding flows
- sign proofs of verification or attestations using cryptographic keys stored and managed in organizational wallets

In such use cases, wallets function not only as repositories of credentials but also as active cryptographic agents, enabling secure and auditable exchanges between organizations and third-party verifiers.

For natural persons, digital wallets serve as privacy-preserving personal data stores, empowering users to retain and control credentials issued by the employers, educational institutions, or government authorities. These wallets provide the following capabilities;

- Enables consent-based disclosure allowing users to selectively disclose only required credential attributes
- Support Cross-boarder portability of employment credentials, which is increasingly relevant in global and remote work context
- Reinforce data autonomy and privacy, eliminating the dependency on centralized intermediaries for identity or qualification
- Maintaining persistent cryptographic proofs and identifiers, ensuring long-term verifiability without repeated credential re-issuance.

7.5.3 Data Minimization and Privacy by Design Compliance with GDPR (Art. 5 and Art. 25)

As seen in the 3.4, the employment verification use case inherently involves exchange of sensitive personal data such as job title, name, date of birth, role duration, and organizational affiliation. However only the minimum set of attributes necessary for a given verification purpose will be disclosed in the proposed solution in accordance with Article 5(1)(C) of GDPR. For instance, a verifier seeking to confirm candidate's job title and employer during a specific time period will not be exposed to unrelated attributes such as a national identification number or full residential address, unless explicitly required for compliance or legal auditing purposes.

This selective attribute release is implemented through VCs conforming to the W3C VC Data Model 2.0 and enriched using selective disclosure and ZKP mechanisms enabled by the walt.id stack. Such capabilities allow the holder to cryptographically prove facts like "Employed as a Software Engineer from March 2022 to May 2025" without revealing unnecessary background data.

By a design standpoint, the system adheres to the privacy-by-design and privacy-by-default principles outlined in Article 25 of GDPR. This is achieved through the integration of DIDs, that enable identification without centralized storage of personal data. Off-ledger credential storage, in non-custodial digital wallets, where users retain exclusive control of their credentials, Consent-driven data sharing protocols, ensuring verifiers only receive attributes that the holder has explicitly approved.

Additionally the architecture aligns with Article 20 (Data Portability) by ensuring that individuals can seamlessly carry their VCs across different employment opportunities and jurisdictions without the need to recreate or resubmit documentation. This is particularly beneficial for cross-boarder employment scenarios, a core focus of our thesis, which require standards-based interoperability and user-driven data mobility.

7.5.4 Privacy and Pairwise Identifiers

Privacy is conceded a vital aspect for individuals in an employment verification system. A key question that we may ask ourselves is whether using did:key for natural persons DID allows the individual to avoid unnecessary correlations between different credentials or interactions. The answer to this is, by design, the did:key gives the user full control to use multiple DIDs if they desire, since creating a new did:key is trivial, a user could use one DID for their diploma credentials, another DID for their employment credentials, or even different DIDs for different job applications. This pairwise identifier approach is recommended in the SSI for privacy, as it prevents verifiers from correlating two credentials just because they have the same subject DID not unless the user wants to present them together. For instance Junior might have [did:key:JuniorWork](#) that he have to his employer when getting his proof of employment history, and a separate [did:key:JuniorUni](#) for his university when getting the diploma certificate. If he applies for a new job, he would choose to present only the diploma credential initially, and the verifier would see only the [did:key:JuniorUni](#)

7.6 User Scenarios and Use Cases

To better illustrate the functionality and applicability of the proposed Employment VC within a real-world organizational context, this section presents two practical user scenarios, one from the perspective of the HR department acting as the issuer, and another from the perspective of an employee as the credential holder. While it is not feasible to capture the full spectrum of potential use cases in domain-specific industries, these two representative scenarios encapsulate the most critical functionalities aligned with the scope of the problem. They provide insights into how the Employment VC can be seamlessly integrated into existing workflows and highlight key operational considerations such as credential issuance timing, employment status updates, and post-employment utility.

7.6.1 Scenarios

Scenario 1: HR Staffs as issuers- Credential Issuance During Employment verification Use Case

Sofia, an HR officer at *Company X* is responsible for managing employment records and onboarding new hires. Her organisation has integrated its HR system with our Employment VC issuer platform. As part of their internal policy, The company issues

verifiable credentials to employees during the course of their employment upon formal request.

When Sofia hires a new employee, the employment data is already stored in the company's Workday system. Through a secure connector, Sofia accesses the issuer portal interface, where a dynamic Employment VC is auto-generated with all the requested attributes. After reviewing the accuracy of the information, she either approves the issuance proactively or responds to a formal VC request from the employee. .

Upon approval, The Employment VC is generated, cryptographically signed by Company X's issuer key, and linked to the employee's DID. The system then offers two secure delivery methods for the credential; Either through a URL link sent directly to the employee (e.g. Via email or employee portal) OR a QR Code, which the employee can scan using their digital web wallet to initiate the credential reception via an OIDC4VCI flow. Once Accepted, the VC is marked with a credentialStatus of Active, indicating valid employment during the ongoing contractual period.

The employment status lifecycle is reflected in the credential's status updates. If Junior is on a legally recognized leave e.g. maternity/paternity or medical leave, the status may be updated to "Suspended" signalling temporary inactivity while retaining credential validity. This allows the employee to continue using the VCs for non-disqualifying purposes such as checks for remote works or freelance engagements during leave.

When an employee exits the company, the VC's status is updated according to terms of the off-boarding process. If the departure is amicable e.g. resignation or contract completion, the VC may remain suspended for a transitional period e.g., three months, allowing continued verification while individual seeks new opportunities. However in cases of termination due to misconduct or policy violation, the VC is promptly updated to "Revoked", rendering it cryptographically invalid for future presentations.

Scenario 2: Employee as Holder, Using Employment VCs

Junior is a software engineer employed at *Company X*. During his tenure, he receives an Employment Verifiable Credential from the company via his web wallet. The VC contains structured claims including his job title, employment type, employer associated with DID, and employment duration (start Date, end Date). The VC also includes metadata such as the issuanceDate, a reference to the credentialStatus, and a link to a schema hosted in Trusted Schema Registry.

The VC is cryptographically signed by the user and delivered to Junior's wallet either as a secure URL or as QR code that can be scanned to retrieve the credential through an OIDC4VCI-complaint flow. At issuance, the credential's status is marked as "Active," enabling its immediate use for employment verification purposes across various contexts such as, verification of employment history for freelance or remote work applications, Background screening by staffing platforms or third-party verifiers, and onboarding processes in new organizations requiring validated proof of roles.

During his tenure, if Junior takes extended leave, the VC's status is updated to suspended, reflecting temporary inactivity without revocation. This allows him to continue presenting the VC in contexts where employment history is relevant but ongoing employment is not strictly required.

Upon leaving the company, Junior's VC remains in suspended status for a grace period of up to three months. This post-employment window allows continued use of the VC in job applications or institutional verifications while offboarding details are finalized.

Figure 24: Caption

Scenario 3: Verifier in Hiring Workflow- Credential Verification at onboarding

Linda, a recruiter at Company Y, is evaluating candidates for a mid-level software role. One applicant, Junior, presents a Verifiable Presentation via OIDC4VP-enabled interface during the application process. The VP includes his Employment VC from Company X containing verified employment data such as job title, employer identity, employment dates and Credential Status.

On the portal Linda receives and processes the VP via a QR code or URL. The presentation is cryptographically signed by Junior's wallet and include the attributes required by the recruiter, ensuring minimal exposure. The system flags the credential's current status to assist in decision-making. In this case, the credential is marked suspended and the verifier interprets this as a recent transition out of the company, within the permissible three-month suspension period.

7.7 Interoperability and Integration with Existing Systems

An important aspect of the analysis for the Employment Verifiable credential is its ability to integrate with existing enterprise systems, particularly human Resource Management systems and other internal data sources used by employers. According to W3C Verifiable Data Model 2.0, the concept of software trust boundaries and credential aggregation are essential when implementing VC-based architectures in real-world environments. These Concepts help ensure that data used for credential issuance remains accurate, privacy-preserving and sourced within trusted systems under organizational control.

In the proposed system, the Employment VC is hypothesized not to be issued manually or in isolation but instead generated through a process of selective aggregation of employment-related data already maintained within the organization's HR systems. This data may include all data attributes included in the low-trust trust model credentials. The feasibility of this model relies on the ability to define trust boundaries around the software components that perform data retrieval and credential issuance. Within these boundaries, the issuer's system can securely access internal data sources and compose the credential payload without unnecessary exposure or duplication of sensitive information.

To achieve this, the system design assumes that issuer portal interface can be embedded into or loosely integrated with existing platforms like SAP SuccessFactors, Sailpoint, workday BambboHR, or custom ERP solutions. This integration is enabled through;

- **Connector-based integration:** These are modular adapters or APIs that allow the credential issuer service to fetch necessary employment data from existing platforms. The design ensures that only authorized systems and users can initiate the data exchange, preserving access control and consent policies from the issuer side.
- **Selective aggregation logic:** Rather than importing a full employee profile, the system pulls only the attributes required by the credential template. For instance, in issuing an Employment VC, the system may aggregate only title, employment period, employment ID, roles served, Competency profile. This supports data minimization principles and ensures the resulting credentials aligned with the specific verification context

- **Template binding and user experience integration** Credential issuance templates that forms the VC card can be embedded in the organization’s administrative interface, prefilled with aggregated employment data. The employer reviews and approves the issuance based on the template card, facilitating seamless workflow integration and reducing duplication of manual data entry.

The W3C VC data model 2.0 explicitly supports this method of claim aggregation, stating that a VC may be composed of claims retrieved from multiple systems, as long as the aggregation takes place within trusted boundaries. This approach enables modular and policy driven VC generation without requiring data centralization or permanent linking of disparate data sources.

Thus, the provisioning of Employment VCs from existing systems is technically and operationally feasible. Organizations can embed the VC issuance and verification workflow into existing platforms using secure connectors and credential interface templates enabling the generation of trustworthy, privacy-preserving credentials based on internally maintained HR data. This design minimizes friction, promotes automation, and supports standards-compliant integration within diverse enterprise ecosystems

7.8 Conclusion of the Analysis

This chapter has systematically examined the traditional CV structure, its associated employment verification artifacts, and mapped them into verifiable components suitable for decentralized representation using SSI and DLT technologies. Through this analysis, we identified which CV claims can be credibly transformed into Verifiable Credentials, distinguished between high- and low-trust credential models, and evaluated the necessary issuer trust frameworks required to support each.

Furthermore, we considered technical, regulatory, and architectural factors essential for enabling scalable, privacy-preserving credential exchange. The outcome of this analysis directly informs the design of our decentralized employment verification system, guiding the definition of credential models, issuer configurations, and data handling strategies.

These insights form the foundation for the subsequent design chapter, where we implement these analytical conclusions into a functional system architecture that supports secure, interoperable, and trustworthy employment credential issuance and verification.

8 DESIGN

This chapter presents the technical design applied into the development and implementation of the system. Built on the foundational principles of SSI enhanced by Walt.id Frameworks, we provide a comprehensive understanding of the architectural components, data flows, trust relationships and integration strategies necessary to implement a scalable and interoperable employment verifiable credential ecosystem.

Addressing current challenges discussed in our introduction chapter 1.2, fragmented verification processes, lack of trust interoperability and reliance on manual verification of claims. This chapter lays out a modular, standards-based architectural reflections from walt.id Framework. Addressing these issues cryptographically, verifiable or traceable credentials claims, decentralized issuer Verification, and the secure data exchange protocols applied in implementation of the solution.

We include service architecture descriptions, micro-service orchestration among the system actors, credential lifecycle management, interaction points with trust registries, and sequence diagrams that illustrate core system interactions which is issuance, presentation and revocation. Special emphasis is placed on the conformance workflow and how walt.id enables practical implementation of open standards discussed in our 7 Chapter. This chapter functions as the bridge between analysis and implementation, it ensures that the system's technical architecture aligns with both regulatory requirements and real-world operational constraints, thus providing the blueprint for secure, interoperable and future-proof employment verification solution.

8.1 Service architecture

The service architecture builds upon the modular and extensible design of the Waltid Framework. This architecture adheres to microservices principles, employing containerization via Docker to ensure portability, maintainability, and scalability across deployment environments. The overall structure is logically divided into three key layers, the application layer, the service layer, and the integration layer.

8.1.1 Application Layer

The application layer provides user-facing interfaces tailored to the three actors in the system, the employer, the employee and the Hiring Company. These interfaces are responsive and designed for cross-platform compatibility both desktop and mobile.

- **Issuer web Portal:** A secure administrative interface through which authorized organizational entities can issue VCs to employee.
- **Verifier Web Portal:** A dedicated interface for verifiers such as recruiters or employment agencies. It enables verification of employment credentials through standard OIDC4VP, and supports selective disclosure mechanism.
- **Holder Wallet(PWA):** A non-custodial, progressive web application that allows individual users to store, manage, and present their credentials. The wallet is fully compliant with SSI principles and supports credential receipt, offline access, DID resolution, and cryptographic proof generation.

8.1.2 Service Layer

The service layer comprises a set of backend microservices, each responsible for the core logic and processing related to its respective actor. These services expose RESTful APIs

consumed by the application layer and other systems components. Each service also leverages shared utility libraries for cryptographic operations, DID communication, authentication, and credential handling,

- The Issuer Services are for;
 - Credential issuance and signing
 - Schema Validation
 - DID binding and metadata creation
 - Also provides integration with HR data sources but this is not implemented
- The holder Services then the following functionalities;
 - Credential Storage and retrieval
 - Presentation generation and consent handling
 - DID key pair management
 - Identity binding and selective disclosure
- Then lastly, Verifier service provide the following functionalities ;
 - Presentation request and consent handling
 - Verifiable Presentation validation
 - Trust checks, issuer authenticity, credential status
 - Consent and audit logging

8.1.3 Libraries and Protocol Support

The architecture integrates multiple libraries and protocols that support SSI functionalities, Core SSI libraries

- Authentication Libraries: Managing secure user authentication and authorization protocols.
- Credential Libraries: Handling creation, storage, and management of verifiable credentials adhering to W3C standards.
- Crypto Libraries: Providing cryptographic operations essential for secure identity and credential management.
- OpenID4VC Protocols and SD-JWT Libraries: Enabling standardized identity interactions and selective disclosure mechanisms.
- DID Libraries: Supporting various Decentralized Identifier methods for secure and interoperable identity representation.

Additionally, the framework offers the SSI-CLI SDK, a command-line interface tool providing developers and administrators powerful, scriptable interactions with the system for management and integration tasks.

8.1.4 Containerization and Deployment

The deployment of these services leverages Docker containerization, significantly simplifying the orchestration, scalability, and maintainability of the system. Each microservice runs in an isolated container, enhancing security and enabling efficient scaling based on real-time demand.

8.1.5 External Integrations

To bolster functionality and user experience, the system integrates seamlessly with external services and technologies, such as:

- Keycloak: Providing robust identity and access management capabilities.
- Authenticator Applications: Supporting secure user authentication processes.
- Database Systems (MongoDB, SQLite): Ensuring reliable, scalable, and performant data persistence and retrieval operations.

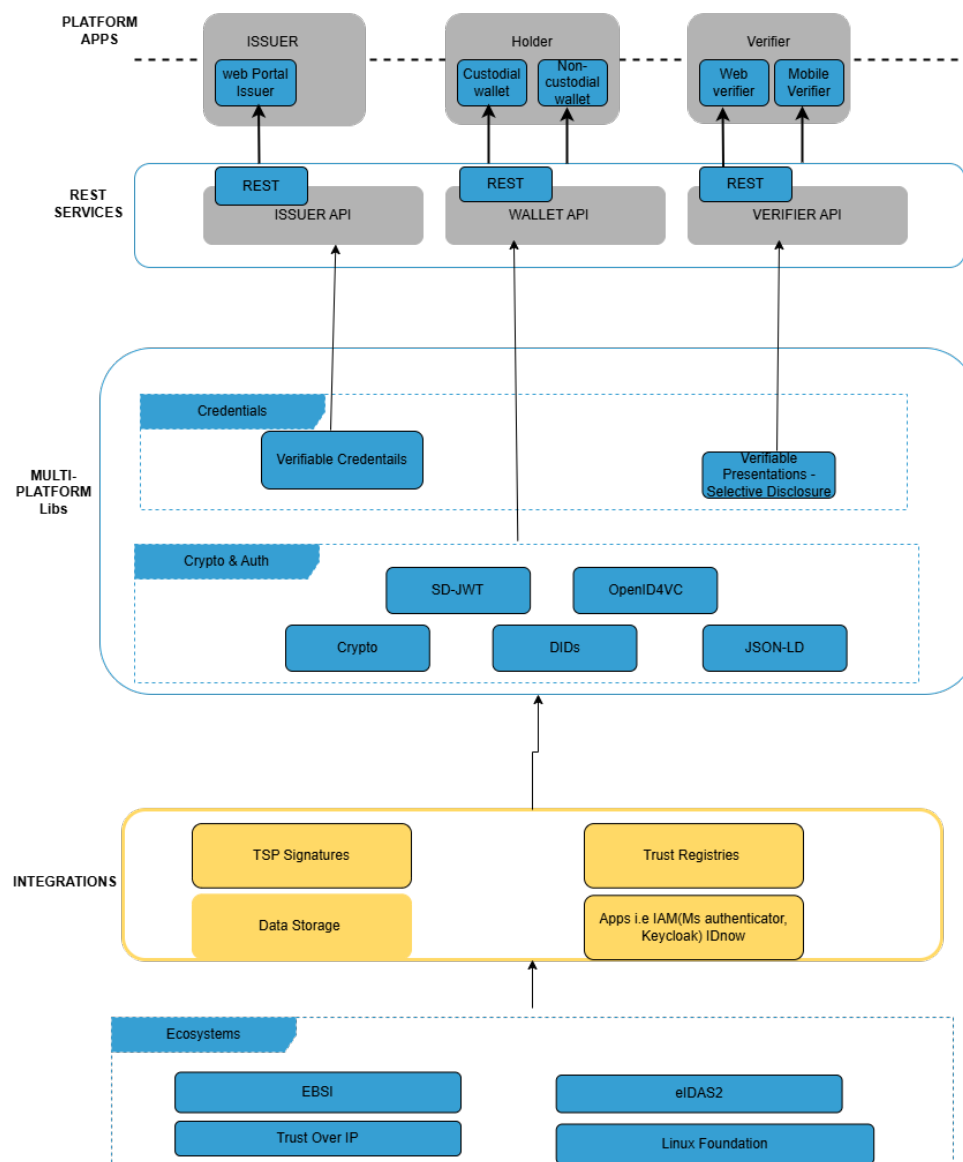


Figure 25: Service Architecture for the design of the Employment Verification

We use `walt.id`'s credential status service to create and manage status list credentials for revocations. It publishes bitstring status list per W3C VC Status List 2021 and token-status-list tokens to record revoked credentials, which the verifier checks during validation. Thus, each microservice has a focused responsibility issuance, presentation, wallet storage, DID resolution, registry sync, revocation, using `walt.id` components under the hood, and together they interconnect over REST. For instance, the issuer service may call the registry sync service before issuing to validate an Issuer DID, or the verifier service queries the Revocation List Manager to check credential status. In operation, Docker containers host each service like `waltid/issuer-api`, `waltid/verifier-api`, `waltid/wallet-api`, plus custom services and a shared network via Docker Compose links them on secure internal interfaces.

8.1.6 API Interfaces

All system services mentioned in ?? expose Https/REST APIs and integrate using OAuth/OIDC flows for verifiable credentials. The Issuer API supports OpenID Connect for VCs issuance. In application it provides standard OAuth2/OIDC endpoints like Authorization Endpoint and Token Endpoints.

The Credential Service handles issuance of VCs supporting formats such as JWT-VC and SD-JWT for selective disclosure. It exposes OIDC4VCI-compliant endpoints;

- */.well-known/openid-configuration,*
/.well-known/openid-credential-issuer
- */par (Pushed Authorization Request)*
/authorize
/token
/credential

Credential offers and issuance sessions are initiated by the holder's wallet, which consumes these endpoints during the credential request process. Issuer authentication and API protection are enforced through keycloak. Then, presentation service initiates and validates VPs submitted by holders. It provides OIDC4VP endpoints to;

- initiate presentation: */openid4vc/verify, /openid4vc/pd/id*
- Manage sessions: */openid4vc/session/id*
- Accept VPs (direct_post): */openid4vc/verify/state*

The wallet API offers secure credential storage and management for the users who are the natural persons. It supports credential receipt, storage and presentations using;

- */wallet/credentials* for list, add, delete
- */wallet/present* for Creation of presentation
- */wallet/authorize* for OIDC4VC credential flow

It integrates SD-JWT and supports cryptographic proof generation. Authentication and consent are handled via keycloak, with users in control of what data to disclose during verification

8.1.7 Technological stack for the Implementation

The system is implemented as a full-stack application composed of a front-end client built with Vue.js running in a Node.js environment and a backend service layer developed in Kotlin using the Gradle build tool. This modular architecture allows clear separation of concerns between user interactions, credential lifecycle management and identity resolution logic.

The frontend Vue.js application serves as the user-facing portal for issuers and Verifiers, integrating with RESTful APIs exposed by the Backend Kotlin services. The Backend handles DID generation, credential issuance, and cryptographic operations. This division ensures that sensitive operations remain server-side while client retain intuitive and responsive interfaces suitable for both desktop and mobile access.

8.2 The Onboarding/ Registration Process for New Issuers

Issuer onboarding is designed to be self-service, standards-compliant, and interoperable. An issuer represents an authorized organization to issue VCs on behalf of a legal entity. The onboarding is rooted in the did:we method, which supports DID creation and publishing via Https without dependency on blockchain anchoring. The following steps outline the issuer onboarding into the system.

- **DID Generation:** we initiate the process using did:web to generate an identifier via the walt-cli tool. The process creates a DID document that includes the issuer's public key, and other metadata. The DID follows the format [did:web:robskytec.local](https://robskytec.local/.well-known/did.json), reflecting the issuer's domain, the domain demonstrated here was based on a local server environment.
- **Hosting the DID Doc:** The DID document is then hosted under the standard path *well-known/did.json* on the issuer's domain. In a development environment, a local server, we used http-server and mkcert, is used to simulate a secure HTTPS hosting at <https://robskytec.local/.well-known/did.json>
- **Key storage and Signing Setup:** The keys associated with the DID are stored in the issuer's keystore, which may be backed by local file-based storage or a key management service.
- **Configuration of the Issuer API** The DID is then configured within the issuer service, either statically via configuration files or dynamically within API requests. This establishes the issuer's authority within the system and ensures that any credentials issued by this entity are traceable to correct DID.
- **Hosting Credential Schema** The issuer may also host a credential schema under their domain to define the structure of their Verifiable Credentials. In our system the Schema of EmploymentCredential is hosted at <https://robskytec.local/schemas/employment-vc-schema.json>. This enables schema validation and supports interoperability across verifiers.
- **Publication of Issuer Metadata** For increased transparency, the issuer can publish a metadata file *issuer-metadata.json* under the *.well-known* directory. This file may include the organization's name, CVR number, jurisdiction, logo, and other claims, which are useful to downstream verifiers.

8.3 Verifiable Credential architecture for Employment Verifiable Credentials

As part of the Verifiable credential architecture, we adopt a structured schema to ensure semantic consistency, interoperability, and validation of employment-related credentials. This schema defines the required and optional claims issued by an employer to the employee. The schema provides a standardized representation of employment relationships and enables third-party verifiers to interpret and validate employment claims across Organizations and jurisdictions.

The schema Governs the structure of the EmploymentCredential, which acts as a tamper-evident and privacy aware proof of an individual's employment relationship with an organization. By enforcing constraints through types, formats and required fields, the schema ensure that all issued credentials follow a uniform structure, facilitating validation, trust propagation and selective disclosure during verification.

The figure 26 below shows its design and attributes;

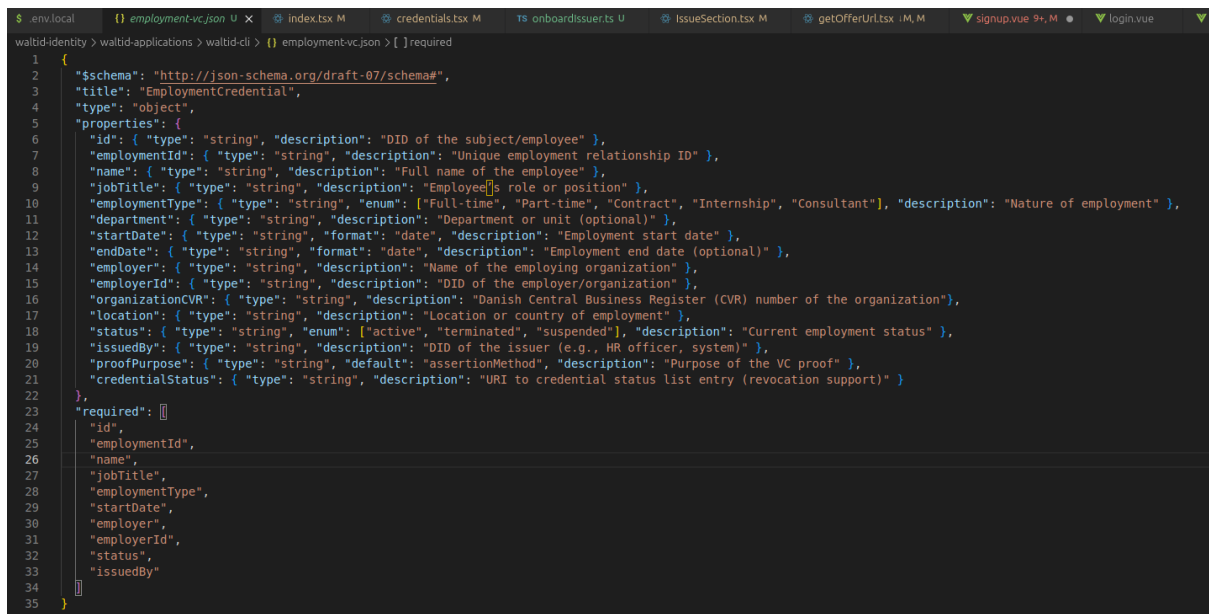


Figure 26: A diagram showing Employment VC Schema and its components

For the system to enforce structured data, each credential type is backed by a JSON Schema. All credential schemas are defined in JSON Schema 2020-12. For instance, the employment credential's JSON schema extends the baseline Verifiable Attestation schema, thereby allowing the incorporation of employment-centric parameters such as employerName, position, startDate. [159].

The implementation of each credential schema requires an associated JSON-LD context facilitating the mapping of specific terms to established definitions or ontologies, which is crucial for maintaining semantic consistency across various systems. Upon the issuance of a credential, the system links this credential's type and schema to the corresponding JSON Schema in the Schemas Registry, which serves as a repository ensuring valid and trusted credentials are utilized.

8.4 Interaction Flows

We detail the end-to-end interaction flows for the proposed system. It follows the OpenID4VC patterns and EBSI trust architecture as described in our analysis Chapter. We describe the credentials issuance flow between the issuer, wallet, and

credential registry, we then describe the presentation and verification flow where holders present VPS to verifiers, the Revocation/ update flows for credential status changes, and lastly, the onboarding process for new issuers/verifiers under the EBSI rule. Each flow highlights walt.id's component and compliance with privacy and EBSI Standards.

8.4.1 Credential Issuance and the binding Process between the employer and the Employee

In our credential issuance setup, the waltid Issuer-api acts as the OIDC Authorization and Resource Server and the wallet-api acts as the OIDC client and DNS/TLS infrastructure provides trusted environment for DIDs and Schemas. The process begins with the wallet initiating a credential request using the issuer's metadata endpoints, followed by OIDC4VCI authorization request. The issuer then resolves the holder's DID through the DID Registry or a publicly available resolvable DID, and retrieves the appropriate schema from the schema Registry within the DNS domain, ensuring interoperability. A W3C-Compliant Employment Verifiable Credential is then created, signed using the issuer's private keys e.g ES256k9 and returned to the wallet via the credential endpoint.

The figure 27 represents the issuance flow that binds the Employer to the employee upon employment verifiable credential issuance.

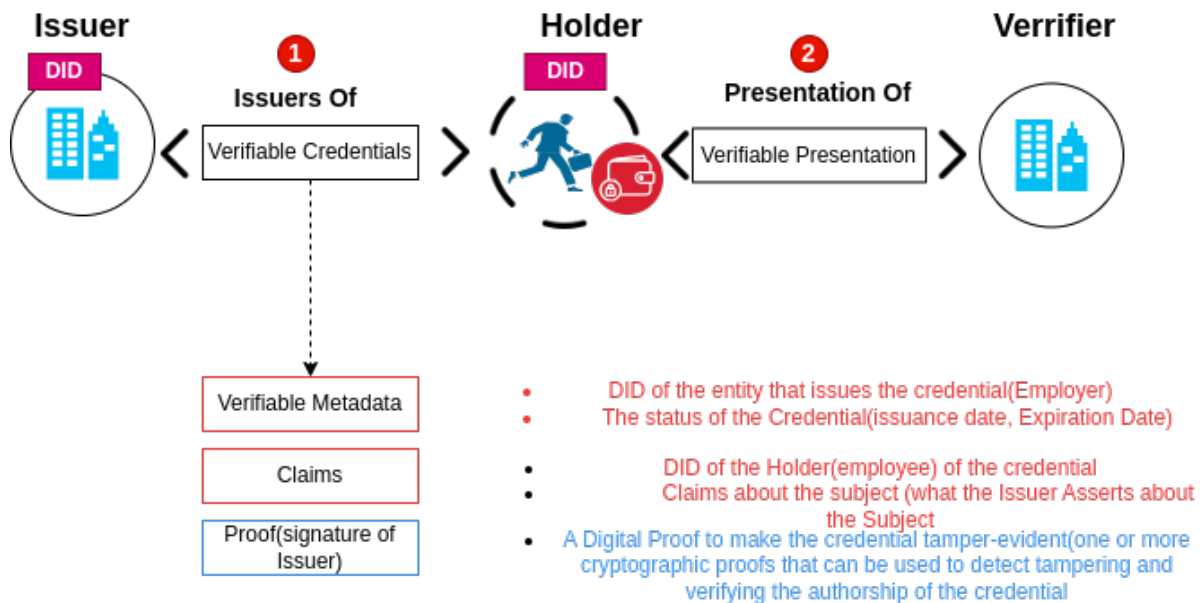


Figure 27: Verifiable credential issuance binding the employer and the employee

The issuer may also register the credential's status like Active using mechanisms like StatusList2021. This process also integrates OIDC protocols with EBSI's trust infrastructure, enabling secure, interoperable issuance of verifiable credentials through standard REST interfaces supported by walt.id.

8.4.2 Presentation and Verification Process Flow

When a holder needs to prove employment, they generate a verifiable presentation using the OIDC4VP protocol. This process begins when the verifier initiates a credential request, typically via a QR code or redirect URL, specifying the required claims in this case

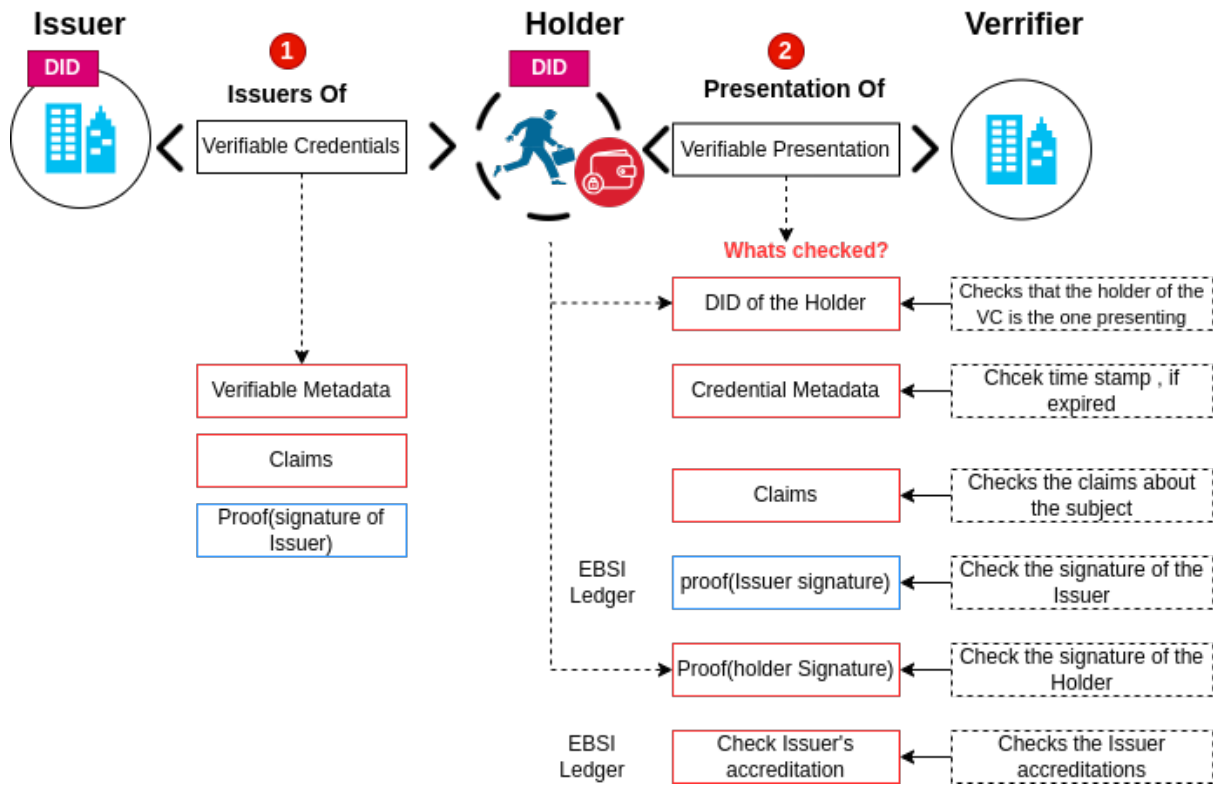


Figure 28: Services Interaction during presentation of an Employment verifiable credential

job title, employment period. The holder's digital wallet via wallet API service receives the request and allows the user to select relevant credentials. A VP is then constructed containing only the necessary attributes, if selective disclosure is used, the wallet includes only the required claims disclosures, preserving data minimization and user privacy.

The wallet first authenticates the verifier by resolving the verifier's DID i.e. did:web or did:key and validating it against EBSI trust chain, ensuring the request originates from a trusted source. Once verified, the wallet signs the presentation using the holder's private key and transmits it to the verifier's endpoint via OIDC4VP protected flow.

On the receiving side, the verifier API validates the holder's DID and signature, verifies the issuer's credential signature, checks the credential schema against the EBSI Schema Registry. If SD-JWT is used, hash comparison is performed to confirm the integrity of disclosed claims. In parallel, the verifier checks the CredentialStatus field via StatusList2021 to ensure that none of the credentials presented are revoked or suspended. This process is efficient and privacy-preserving, as it avoids direct online queries for each credential.

Once all verifications pass, the verifier makes an authorization decision based strictly on the requested claims, ensuring compliance with data minimization and user consent principles. The entire flow is anchored in open standards as mentioned and is governed by EBSI trust infrastructure, ensuring secure, interoperable, and privacy-preserving verification of employment credentials.

The Figure 28 depicts the holder and the verifier backend interaction during the process of Verification. It illustrates key checks that take place before the verifier validates that in deed the issuer of the VC and the holder are authentic

8.4.3 Revocation/update Flow

Credential status in the system is managed using the W3C StatusList2021 mechanism, which encodes revocation status as a compressed bitstring. In this flow, when an issuer either issues or revokes a credential, the corresponding bit at the credential's index in the status list is updated e.g set to "1" for revocation. This change is then published to the issuer's own registry via walt.id's credential-status endpoint. The Updated status list is itself issued as a verifiable credential, containing the bitstring that represents the status of multiple credentials. This is supported by the CRUD operation on the application layer.

8.5 Sequence Diagrams

8.5.1 The Authentication and registration sequence Employee Wallet

The sequence diagram below shows how the holder interacts with the wallet at first

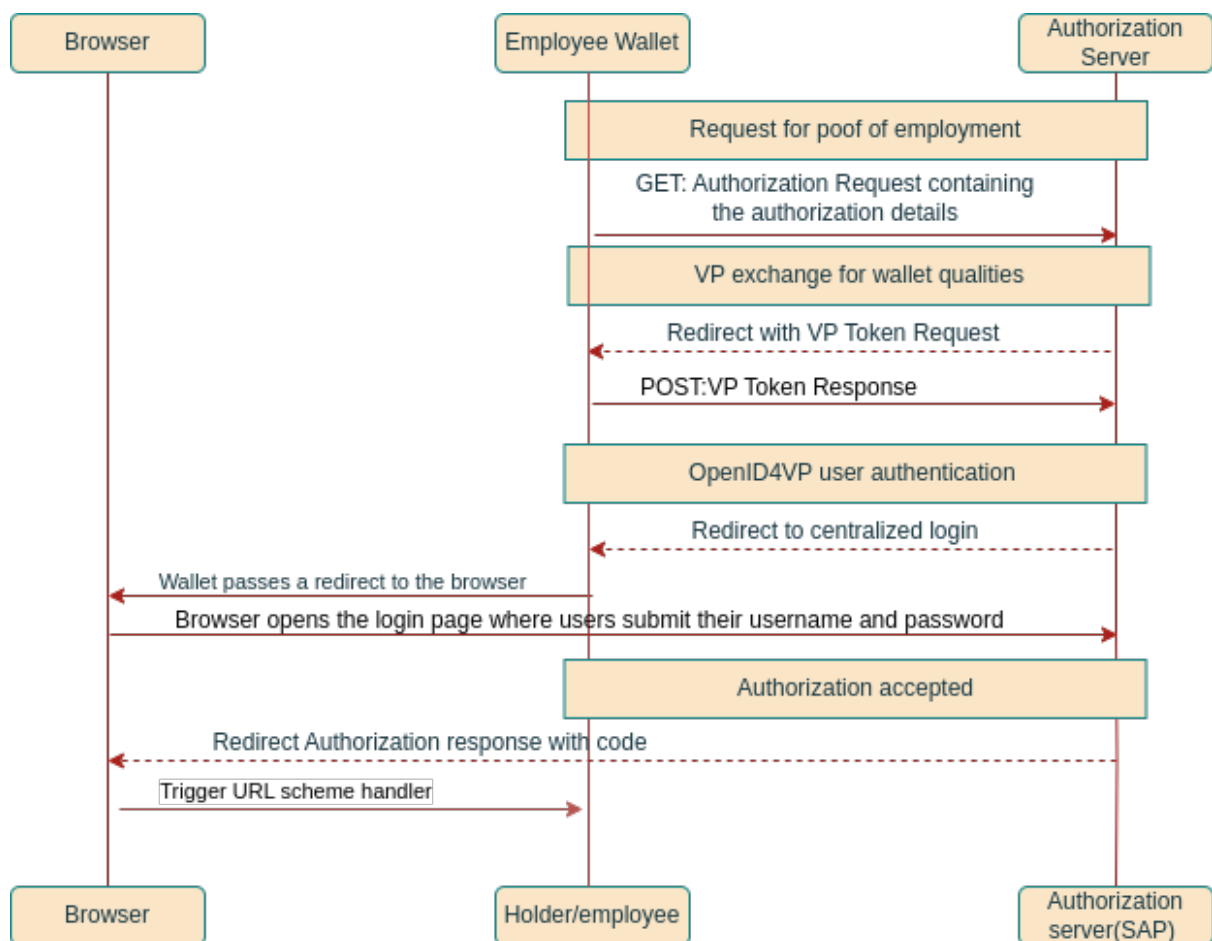
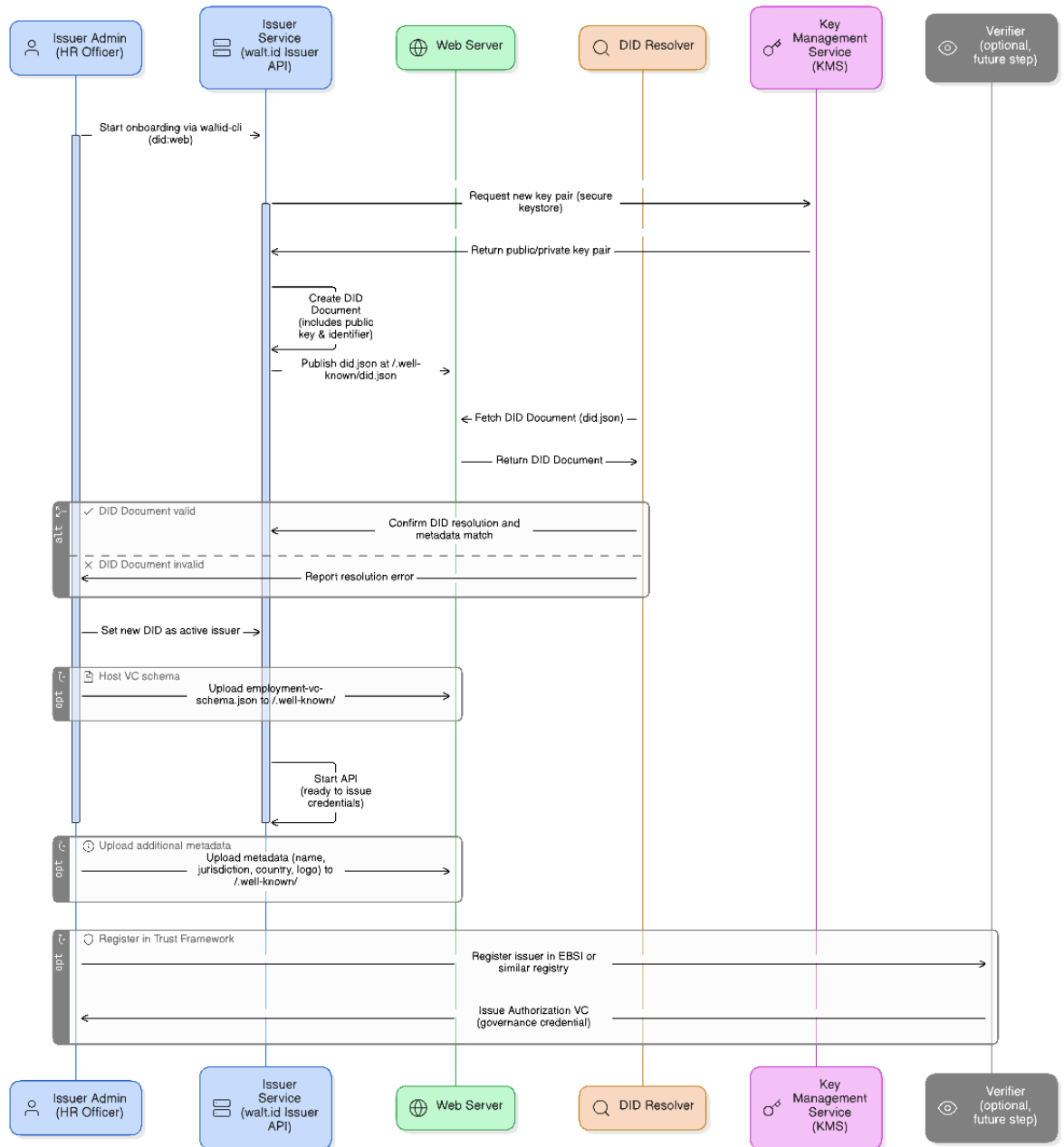


Figure 29: This shows the authorization into the holder wallet

8.5.2 How to Onboard an Issuer Sequence Diagram

The sequence of this well illustrated in the interacting flow thus the sequence of the onboarding process illustrates the process by which a new issuer gets access to the system and issue verifiable credentials.



eraser

Figure 30: Sequential process of the issuer onboarding and Registry operations

8.6 Security and Privacy Consideration

In order to ensure robust protection of user data and trust integrity, the design incorporates multiple security layers spanning from credential cryptography, identity key management, and Decentralized storage design

8.6.1 Cryptographic Proof Mechanisms

In the context of low-trust credentials we adopt a decentralized trust approach that leverages DID methods such as `did:web` and `did:key`. Unlike the centralized,

high-assurance model exemplified by EBSI, our model enables issuers to establish their credibility and manage their cryptographic keys independently, using domain-level trust infrastructures such as TLS and DNS.

Using the `did:web` method, credential issuers anchor their decentralized identifiers to web domains under their control. Trust is derived from the domain's existing HTTPS certificate and DNS infrastructure, which provide verifiable evidence of ownership and control. For example, an employer with the domain `robskytec.local` may publish its DID document at `https://robskytec.local/.well-known/did.json`, which includes its public keys and service endpoints. This setup allows verifiers to validate signatures by resolving the issuer's DID against a trusted TLS connection, ensuring the authenticity of the public key used for credential signing.

In scenarios where issuers do not require public discoverability or domain-bound trust anchors, the `did:key` method is employed. This method generates the DID and associated key pair locally, embedding the public key directly in the DID string. This approach is ideal for use cases such as internal endorsements or project-based employment attestations where rapid setup and peer-level verification are prioritized over centralized authority endorsement.

In both methods, issuers are the controllers of their DIDs. They are solely responsible for the generation, storage, and lifecycle management of their cryptographic key pairs. Signing keys are secured using local cryptographic modules or integrated key management systems (KMS), such as HashiCorp Vault, AWS KMS, or platform-specific HSMs. This key autonomy enables decentralized issuers to operate securely without relying on centralized registration or onboarding processes.

Credentials and verifiable presentations in the system are signed using these cryptographic keys, ensuring data integrity and provenance. Verification is performed through standard asymmetric cryptographic mechanisms, where verifiers use the issuer's DID document to retrieve the public key and validate the credential's signature.

This decentralized proof architecture supports the flexible and scalable issuance of employment credentials across multiple trust levels. It also adheres to established cryptographic guidelines such as those from ETSI, ENISA, and NIST for secure key management and digital signature practices.

8.6.2 Employee wallet solution for Data storage design

In our prototype, the identity wallet is non-custodial, meaning meaning user generate and store cryptographic keys locally on their devices rather than with a central service. Keys are generated using secure random number generator and are never transmitted or stored in plaintext. once generated, private keys are encrypted and stored securely , accessible only by the user through User name and Password.

Wallet app stores the encrypted key locally, never transmitting it to server, ensuring data protection by design. Key recovery, if needed is performed by the user without compromising control. Importantly, no server-side secrets are involved. The blockchain is used for public references only e.g DIDs, credential schemas, and revocation registries, while credential schema contents remain off-chain and encrypted. This on-chain/off-chain separation aligns with GDPR data minimization principles, where personal claims stay encrypted and can be updated or deleted off-chain without altering blockchain records.

By choosing non-custodial wallet we maximize user autonomy, ensuring that users control signing and presentation of credentials without revealing secrets to any server. The design ensures privacy and security while supporting decentralized goals, as emphasized by walt.id, which promotes putting users in control of their data. Issuer public keys are

managed via did:web method, providing secure and access for verifiers without needing blockchain lookups.

8.6.3 Key Management Autonomy After Accreditation

- **Periodic key Rotation for Risk Mitigation**

Issuers are encouraged to rotate their signing keys on a frequent schedule approximately every 60-90 days. regular key rotation limits the window of vulnerability if a private key is ever compromised and reduces long-term cryptanalytic risk. EBSI supports updating cryptographic keys regularly without impacting verifiers because verifiers always retrieve the correct historical DID document from the ledger. An issuer would generate a new key pair and add it to its DID Document through the DID registry API, then begin signing new credentials with the new key and can only later retire the old key. Best practice security literature advises rotating keys roughly every 60 days to ensure trust relationships remain resilient: By rotating keys an issuer bonds the number of credentials signed with any one private. I.e if an issuer normally issues hundreds of credentials per year, rotating every two months means a compromised key would require re-issuing far fewer credentials.

- **DID Resolution and Historical Continuity**

A core advantage of decentralized systems is that it preserves the full history of each issuer's DID Document, ensuring verifiers can always resolve the correct public key of any credential. The DID registry is time aware, every key addition, revocation or expiration is stored with a timestamp, and any DID resolution request can specify a *Valid at* time parameters. This means that even after an issuer rotates keys or revokes an old key, verifiers can retrieve the version of the DID Document that was valid at the credential's issuance time. For example, a verifier checking a year-old VC can resolve the issuer's DID as of that issuance date and obtain the old public key needed to validate the signature.

this backward compatibility is essential for historical verification, and is intrinsically handled by the EBSI ledger. This is captured in the system as Event logs that represents the transactions carried out per user.

- **Multiple Active Keys per Issuer DID**

The DID method for legal entities explicitly allows an issuer to maintain multiple active public keys under the same DID. In the DID Document, these appear as multiple *verificationMethod* entries. Operationally this enables smooth key rotations and role separation. For instance, an issuer can add a second signing key before revoking the first, allowing a brief overlap where both keys are trusted. Verifiers will accept signatures from any current key in the DID Document, so there is no service downtime during rollover. Multiple keys also permit separating concerns e.g., one key used for routine credential signing and another the key management used exclusively for updating the DID document.

8.6.4 DID Documents and verifier Interaction

On the verification side, an employer or other relying party performs standard VC checks plus trust chain checks. First, the Verifier resolves the issuer's DID Document from the EBSI DID Registry; no special permission is needed for reads. The DID

Document, which is stored on chain at the registration, contains the issuer's public keys and controller information. In particular, the *assertionMethod* The key in the DID Document is used to cryptographically verify the signature on any VC the issuer present. Next, the verifier examines the credential's metadata. It checks the schema ID, issues data etc., and crucially it inspects the *termsOfUse* attestation policy field. That field contains a reference a URL into the TIR that links to issuer's own accreditation and indirectly to the TAO's authorization. The verifier can retrieve the referenced credential from the TIR or call the EBSI credential status API to confirm that the issuer's accreditation is still active. In effect, the verifier checks the blockchain to ensure that the presenting issuer is indeed listed as a trusted issuer for the credential type. All of these checks, DID resolution, signature verification, and TIR lookup are handled by the verifiable credential libraries in the wallet.ID Verifier SDK in a standard way.

9 IMPLEMENTATION

This chapter presents the practical implementation of the decentralized employment verification system, translating the design and architectural models discussed in previous chapters into a working prototype. Core components are developed using the Walt.ID SSI framework, integrated with EBSI-compliant services to ensure trust interoperability.

The implementation follows a microservice-oriented architecture, with modular services for credential issuance, presentation verification, revocation handling, wallet management, and registry integration. The prototype also showcases the incorporation of privacy-preserving mechanisms in alignment with regulatory requirements.

9.1 Web Wallet Application

The web wallet application functions not merely as an interface, but as a personal digital ecosystem for natural persons, enabling the secure storage, management, and controlled disclosure of VCs and DIDs. It consolidates various aspects of an individual's digital identity, such as employment attestations, educational qualifications, and regulatory certifications, into a self-managed, interoperable container. Within the employment verification context, this wallet serves as the holder's agent with the capacity of a CV, allowing them to present cryptographically verifiable proofs of their attributes to potential employers, staffing agencies, or regulatory bodies.

9.1.1 Authentication interface/Sign In

Upon accessing the application, users are directed to a secure authentication interface, which supports multiple login mechanisms. Holders can either register using an email and password pair, authentication through decentralized and federated identity options; SSI login using Ethereum-based DIDs, enabling identity binding without relying on centralized credentials, OpenID Connect authentication allowing users to connect using trusted external identity providers in line with OIDC standards.

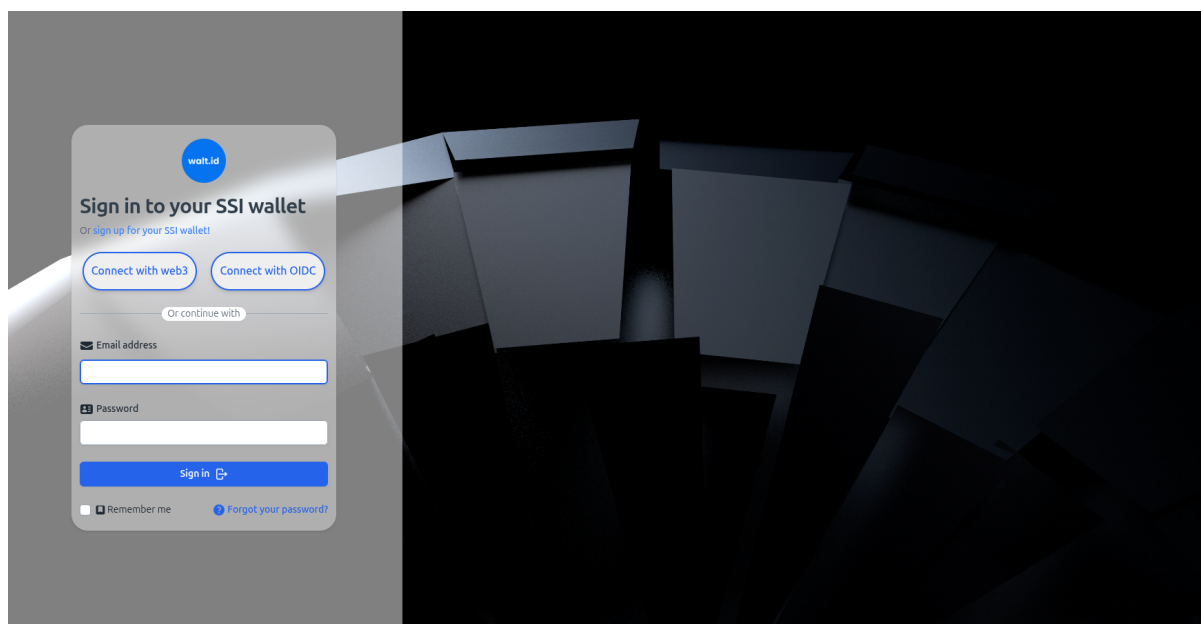


Figure 31: Web wallet User Sign In Interface

Figure 31, shows the user sign in interface for the holder

9.1.2 The User Profile Interface

The wallet automatically generates a cryptographic key pair and assigns a DID to the User as shown in 32. This DID acts as a persistent, verifiable digital identity anchored in the EBSI trust infrastructure, and it enables the user to receive, present, and sign verifiable Credentials using their own private key. This process aligns with the DID core specification and is implemented via Walt.ID's DID libraries, with support of did: key methods.

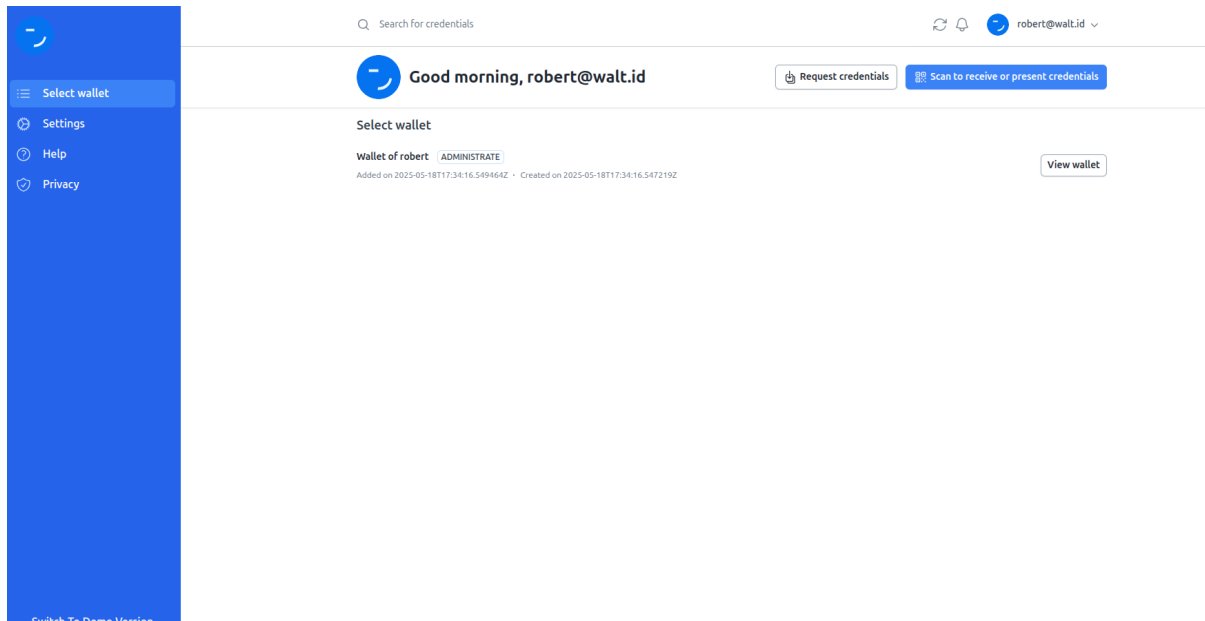


Figure 32: wallet DID interface and management

9.1.3 Credential Management interface

This interface allows users to receive, view, store, and delete VCs issued by trusted parties. Credentials are stored securely in the wallets local vault, and users can initiate presentation sessions to verifiers by selecting specific credentials and choosing which attributes to disclose.

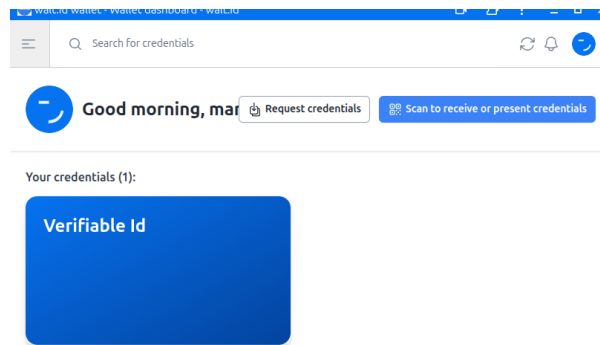


Figure 33: Credential storage and management on the employee wallet

9.1.4 DID Management Interface

Through the DID management panel, users can generate new DIDs for different purposes and credential issuers, participate in multiple trust ecosystems, or rotating keys for security. Each DID is associated with a key pair and a DID Document, which is either published on or resolvable through an EBSI-compliant DID registry. This interface empowers the user to maintain full control over their digital identity, including key lifecycle operations

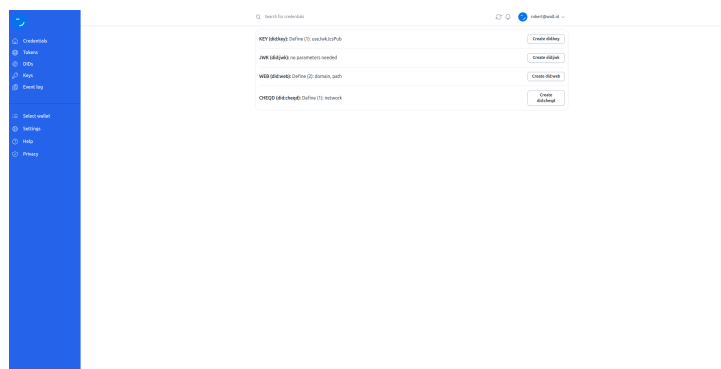


Figure 34: DID methods within the wallet

9.1.5 Event Log Interface

For transparency and auditability, the wallet includes an event log interface, which records critical identity and credential-related actions. These include credential issuance, revocation, presentation transactions, DID registrations, and consent events. Logs are stored locally and can be exported for compliance allowing users to track how and when their credentials have been used or shared. See figure 35 Below

Event log
The list of events is shown below:

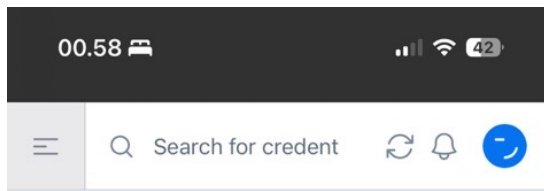
List of events

TIMESTAMP	EVENT	ACTION	TENANT	ORIGINATOR
2025-06-01T20:50:29.063615Z 000004	Key	Create		wallet ***
2025-06-01T20:50:29.095809Z 000004	Did	Create		wallet ***
2025-06-01T20:50:29.103152Z 000004	Account	Create		wallet ***
2025-06-01T20:50:57.842239Z 000004	Account	Login		wallet ***
2025-06-01T22:19:27.928814Z 000004	Credential	Receive		***

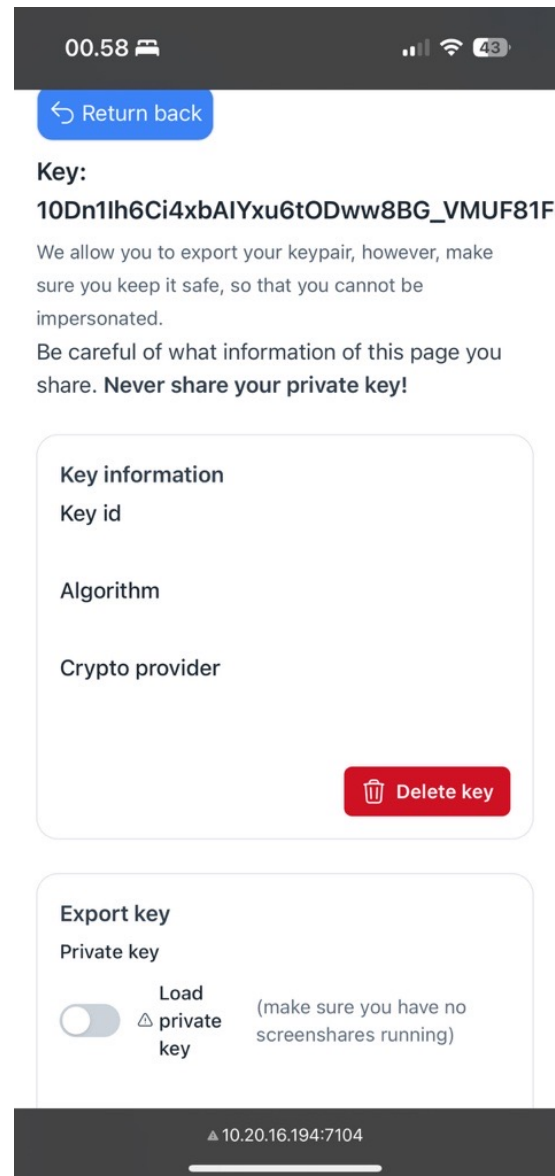
Figure 35: Event logs of transaction in the Wallet

9.1.6 Key management Operations

The wallet includes a comprehensive key management module to support secure and user-controlled identity operations. Upon onboarding, users can generate cryptographic key pairs, which are the used to derive did:key, did:web identifier. these keys are stored securely within the wallet, with options to view, export, or delete them. The wallet supports signing and verification functions , enabling



(a) new key creation



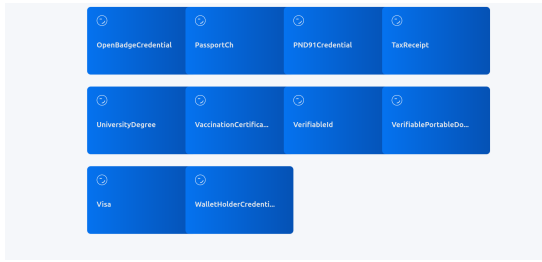
(b) Key management

Figure 36: Public private key management in a wallet

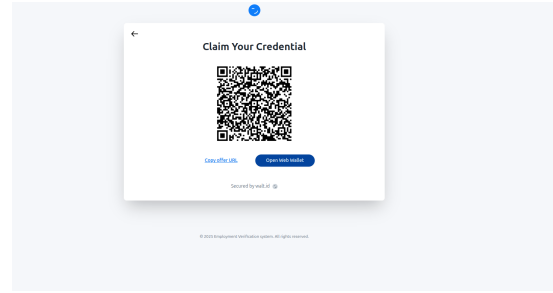
9.2 Issuer and Verifier Web Portal

9.2.1 Issuer portal

The issuer portal shows the interface used by an issuer, HR staffs select a template, from the different VCs on the portal and click a start button to start the process of issuing Employment verifiable credential. This triggers a prompt page with a QR code and a copy link that enables issuance of the VC to the employee



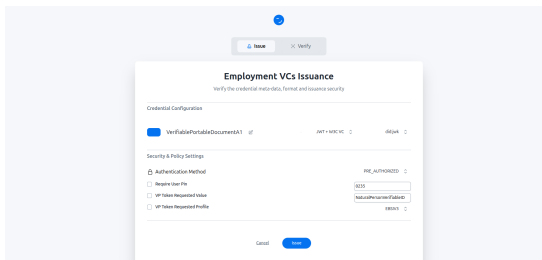
(a) Issuer Portal interface



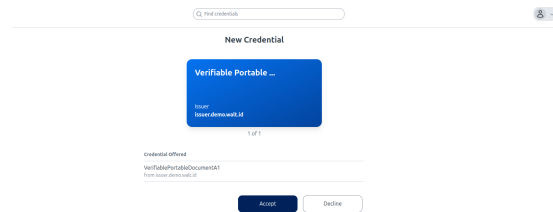
(b) Issuance of a VCs

Figure 37: Employment verification issuance User Interface

The credential is then Sent to the Issuer wallet as depicted in the Figure 38 below



(a) Credential Details

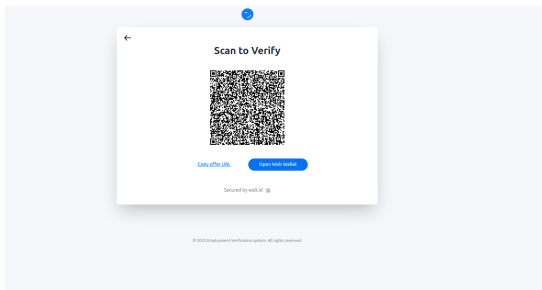


(b) Consent Management of the Credential

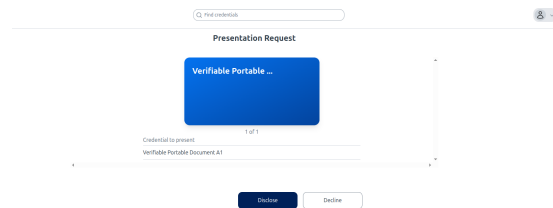
Figure 38: Consent and receiving of VC in a digital wallet

9.2.2 Verifiable presentation

Lastly this figure illustrates the implantation of the presentation of a VP to a verifying third-party, where holder can scan a QR code or link sent to him/her and then consents if they want to verify or disclose the require information



(a) VP Presentation



(b) Consent to disclose VP

Figure 39: Verifiable presentation of Emloyemnt Credential

10 DISCUSSIONS

In practice, the relevance of this system was underscored by a company that acknowledge recurring incidents where job applicants provided misleading information about their past employment, including exaggerated job roles, and a falsified reference. These real-world cases validate the core motivation behind our project, namely that traditional employment verification is susceptible to manipulation and lacks scalable trust mechanisms. The proposed system, grounded in VCs and DIDs, directly addresses this vulnerabilities by enabling employers to cryptographically issue proof of employment roles and durations. The company recognition of the system's potential impact provides additional confidence in both the problem framing and the utility of our solution in real-world hiring workflow.

Additionally, a key insight is that employment credentials can be effectively anchored in a trust framework that combines issuer DIDs, trusted schema registries, and revocation mechanisms. This addresses the first research question by demonstrating that verifiable trust relationship between employer and employee can be established through digital signatures, identity binding via did:key or did:web, and issuance policies backed by issuer onboarding protocols. The second question that relates to verifying the trustworthiness of employee provided data was addressed through the implementation of presentation flows OIDC4VP that allow third-party verifiers to validate credentials without interacting with the issuer.

In response to the third question, The Employment VC schema encapsulates job title, tenure, employment type, supervisor, role description, key CV attributes that lend themselves well to machine-verifiable structures. However, elements like personal statements and design aesthetics remain outside the scope of automation, emphasizing the hybrid nature of trust in hiring decisions. Finally this work confirms that initiatives like EBSI and walt.id framework offer mature, interoperable components that accelerate adoption and ensure compliance.

Importantly, while the system delivers significant trust and efficiency improvements, it currently operates in a stand-alone context with no direct HR system integration or live production deployment. As such, its potential impact will depend on future efforts to expand ecosystem interoperability, enhance user experience, and ensure regulatory robustness.

This discussion positions the project as a foundational step toward decentralized career credentialing, while acknowledging that employment verification is a multifaceted process that may always retain some reliance on human judgment, context, and institutional trust.

11 CONCLUSION

This project set out to explore how a decentralized trust framework, incorporating SSI and DLT, could be applied to partially automate the employment verification process, particularly with respect to CV data, while improving trust, privacy and efficiency in hiring. The design and implementation of a verifiable credential system, centred on an Employment verifiable credential, have demonstrated that this goal is both technically feasible and practically relevant within the current digital infrastructures.

First, the project addressed the critical issue of establishing verifiable trust between the employer and the employee by utilizing DIDs, cryptographic proofs, credential status registries. These mechanisms allow for secure issuance, presentation and revocation of credentials without relying on centralized intermediaries. Second, the system design

ensures that the authenticity of the employment data presented by users could be independently verified by third-party verifiers enhancing trust in the hiring process while preserving user privacy through selective disclosure and off-chain data handling.

Third, the project analysed which components of the traditional CV could be represented as verifiable credentials. The Employment VC captures structured, verifiable claims such as job title, role, tenure, and employer identity, while recognizing that more subjective or unstructured elements like soft skills, aesthetic formatting, or emotional intelligence, remain outside of automated verification. Lastly, by aligning with existing ecosystem like EBSI, the solution demonstrates how decentralized employment verification can be incrementally adopted and interoperable scaled.

In Conclusion, this work shows that low-trust credentials, when issued within a standards-based trust architecture, can serve as reliable building blocks for a decentralized employment history ecosystem. Although the current system does not integrate with legacy HR tools or support end-to-end automation, it lays a strong foundation for future extensions. The findings suggest that verifiable credential can reduce friction in employment verification workflow, offer great user agency, and pave way for more trustworthy future in digital hiring practices.

12 FUTURE WORKS

The project demonstrates the feasibility of decentralized employment verification using SSI and DLT technologies, several areas remain open for future development and enhancement. One key direction is integrating issuer onboarding directly into the user interface, replacing the current CLI process with a more user-friendly and secure portal for organizational registration and configuration. Additionally, the system would benefit from integration with existing HR systems through standardized connectors, enabling automated population of credential templates from trusted internal records and reducing manual HR input. Enhancing the issuer interface across both the issuer verifier portals and the wallet portals remains essential, with focus on usability, accessibility, and guided interactions to support both technical and non-technical users.

Performance benchmarking and optimization should be conducted to assess system scalability and responsiveness, particularly in high volume issuance and verification scenarios. Moreover, formal security and privacy testing, including penetration tests, threat modelling and GDPR compliance assessments, will be critical before production deployment. Finally, the system can be extended to support additional verifiable credentials such as reference letters, and project portfolios, allowing for more comprehensive digital career identity and seamless interoperability within the broader trust ecosystem like EBSI

A Appendix I

A.1 Requirement Specification

The requirement specification section of this project using decentralized identity principles must articulate both the functional and non-functional requirements necessary for the development of the PoC. A clear classification into 'Must have', 'Should have', 'Could have', and 'Won't have for now' designations using the MoSCoW methodology ensures clarity for system architects and technical contributors, addressing the specific needs of stakeholders engaged in or impacted by this project.

A.1.1 Functional Requirement Specification

The functional requirement as is in Table 3 focuses on essential features that must be implemented for the solution to be viable. This includes the ability to handle user identities securely through DIDs that comply with the European Union's GDPR and eIDAS 2.0 directive. Articulating stakeholder needs clearly is critical for accurate requirements analysis, which helps mitigate issues in design and implementation. Furthermore, the need for effective requirements verification is emphasized; the verification process must confirm that these functional requirements align with broader project objectives without introducing ambiguity or inconsistency, as identified by [79].

ID	Requirement	Description	Priority
FR1	DID Generation	The system must support creation of DIDs for Issuers, holders, and Verifiers(e.g did:key,did:ebis).	Must
FR2	VC Issuance	Trusted issuers must be able to issue employment verifiable credentials to holders using cryptographic signatures	Must
FR3	VC Presentation	Holders must be able to selectively disclose credentials to verifiers using a wallet	Must
FR4	VC verification	Verifiers must validate authenticity, issuer trust status, and credential integrity	Must
FR5	Revocation Status Check	The system should support revocation registry lookups to determine credential validity.	Should
FR6	Credential Schema Definition	The system must define a standard schema for Employment VCs aligned with W3C Data Model 2.0	Must
FR7	interoperability with EBSI	The system must integrate with EBSI's trust and DID resolution infrastructure.	Must
FR8	Consent Management	holders should explicitly control when and to whom credentials are disclosed	Should
FR9	Trust Registry integration	Issuers and Verifiers must be discoverable via EBSI's Trust registry.	Must
FR10	Credential Expiry and Metadata	Vcs should include metadata such as issuance/expiry dates, job duration, and issuer details	Should
FR11	Multi-Language credential Support	the VC format should allow for multilingual data attributes	Could
FR12	Cross-Border verification Logging	The system could log cross-border verification events for auditability (non-identity)	Could
FR13	Mobile Wallet support	The system should support mobile-based holders wallets	should
FR14	Cross-Domain Issuers support	The system could allow different types of issuers like employers, social security	Could
FR15	Role-Based Access Control (RBAC)	The Issuers and verifiers must support RBAC for administrative control	Must
FR16	Issuer Wallet interface	Issuers must have access to a wallet dashboard or API for issuing Credentials	Must
FR17	Verifier API	Verifiers must access a VC verification API for automated credential Checks	Must

Table 3: Table showing the functional requirements of the system

A.1.2 Non-Functional Requirements Specifications

Non-Functional requirements encompass constraints and quality attributes that the PoC must satisfy. Privacy, interoperability, and usability are paramount in this context. There are potential challenges in requirements structuring that could hinder effective verification, particularly when user data privacy is involved. Traditionally, the transition to verifiable credentials necessitates robust user experience protocols that enhance usability while ensuring compliance with regulatory mandates, reinforcing the need for quality-focused verification practices as discussed in various studies[79]. As depicted in table 5 the list entails specific behavioural expectations but not limited to the provided as the list can further be adjusted if further development would be required

ID	Requirement	Description	Priority
NFR1	Compliance with GDPR	Personal data must be processed with informed consent and privacy by design	Must
NFR2	eIDAs 2.0 Alignment	The system must align with eIDAs 2.0 for trusted digital identity and qualified issuers	Must
NFR3	VC interoperability	The system must be interoperable with other EBSI-based and EUDI wallet solutions	Must
NFR4	Security	All credentials and communications must use end-to-end encryption and digital signatures e.g., encryption,signature,Authentication	Must
NFR5	System Modularity	Micro-services should be modular to allow future scaling or replacement of components	Must
NFR6	Performance	credential verification should be completed within a few seconds	Should
NFR7	Auditability	The system credential events should be auditable for compliance and governance	Should
NFR8	Availability	The core services like wallet, registry APIs must be highly available	Must
NFR9	Accessibility	The wallet interface and portals should be accessible per WCAG 2.1 standards	Could
NFR10	Usability	Wallet UX must be intuitive to support non-technical users (holder and HR staff)	Must
NFR11	scalability	While full scalability is out of scope, the system should be architected to allow scaling Post-PoC	Should
NFR12	Testing and Validation	Automated test suites should be created for issuance, verification and DID resolution	Should
NFR13	Documentation and Version control	APIs and VC schemas must be well-documented and versioned for future interoperability	Must
NFR14	Legal Traceability	Credential metadata must allow verifying legal origin and status of the issuer	Must

Table 5: Non-Functional requirements table

Core components of Trust Models

In domain such as digital identity, employment verification and SSI environments, trust models typically provide the semantics and mechanisms necessary for evaluating and operationalizing trust[137].

Component	Description
Truster	The Entity that places trust in another, often in a SSI ecosystem is a verifier who needs to determine whether to accept a digital credential e.g., an employer,HR platform, or regulatory
Trustee	The entity trusted, typically the issuer of the credential such as employer, university or professional certifying body.The trustee is responsible for the accuracy and authenticity of the issued claim
Trust Context	The situational domain in which the trust decision is made such as type of the hiring process, a background check, or cross-boarder credential validation. Context heavily influences trust criteria[137]
Trust Metrics	The quantifiable attributes used to assess the trustworthiness of the credential or its issuer.Examples include digital signatures, governance compliance, credential schema adherence and issuer reputation [56]
Trust Decision	The outcome of the trust evaluation process.This may involve accepting the credential as valid, rejecting it due to mismatches, or red flags, or performing additional verification steps e.g., querying revocation registries or issuing a challenge request.
Trust Propagation	The process by which trust extends or cascades through a network of n´relationships, for instance, when a verifier accepts a credential from an issuer based on trust in a shared governance framework,consortium membership, or registry e.g EBSI,Sovrin, or W3C trust registries. Trust propagation is critical for scalability and interoperability

Table 7: Components of Trust Models

Each of the components in table 7 above plays a distinct but interdependent role in building resilient, decentralized trust architectures.In decentralized identity systems, these roles are increasingly formalized through technical standards such as DIDs and VCs [163].Furthermore, governance frameworks as seen in the initiatives like Trust over IP foundations, define the rules, assurances, and protocols that regulate how trust is assigned, evaluated and revoked in a given ecosystem [103].

By integrating these core components, trust models not only support secure exchange of credentials but also facilitate privacy-by-design, data minimization and interoperability, which are increasingly demanded by regulatory and technical standards in digital credential systems.

A.2 Verifiable Credentials non-normative understanding

A.2.1 Definitions of Terms

Claims: On the other hand, statements made by an issuer about a subject, asserting one or more attributes or properties associated with the subject. a In traditional terms, claims are analogous to the information printed on diploma,ID card or employment letter, such as name, dat of birth, job title or education degree.

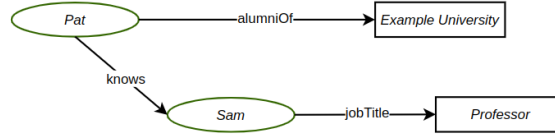


Figure A1: Verifiable Claim

As depicted in figure A1 individual claims can be merged together to express a graph of information about a subject. They are then expressed in JSON-LD format and are found with the `credentialSubject` field.

A.2.2 Verifiable Credentials Data Model

- **Embedded Proof Mechanism**

In the W3C VC framework, the use of embedded proof represents a mechanism for ensuring the authenticity and integrity of credential data. According to the verifiable credential Data integrity 1.0 specification[174], a VC with an embedded proof is structurally composed of at least two distinct information graphs, both expressed in Resource Description Framework (RDF) format as shown in figure A2

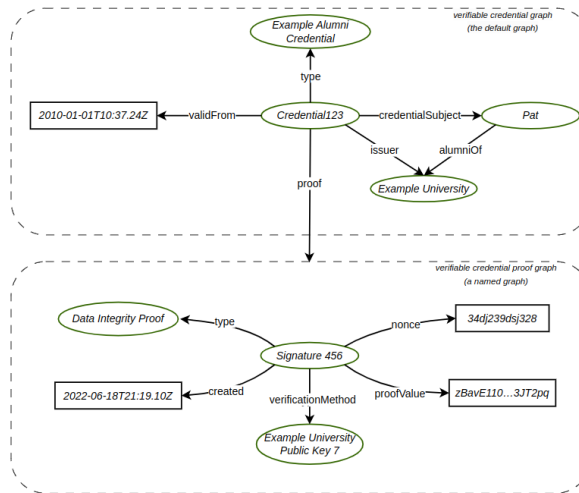


Figure A2: Embedded Proof Mechanism

The first graph, known as the verifiable credential graph, the default graph, contains the core content of the credential. These include metadata such as the credential type, issuer, issuance data and the claims made about the subject.

The second graph identified through proof property, is referred to as the proof graph. This is a named graph that contains the cryptographic proof typically a digital signature generated using the issuer's private key. The presence of a separate graph allows for a clear separation between the content of the credential and the cryptographic evidence used for verification enabling verifiers to evaluate trust without altering the credential's semantic content.

- **Enveloping Proof**

Defines how secure media types expressing VCs and VP using approaches defined by JOSE, OAuth, and COSE working groups at the IETF. This includes JSON Web Signatures, Selective Disclosure for JWTs. they use content types to distinguish between the data types of unsecured and secure documents in conformance with W3C VCs standards. this documents and their associated media types rely on JSON-LD which is an extensible format for describing linked data. The VCs Data model describes the approach taken by this specification to secure claims by applying an enveloping proof where the payload contains a single information graph which is the VCs graph containing credential metadata and other claims as shown in figure A3 below

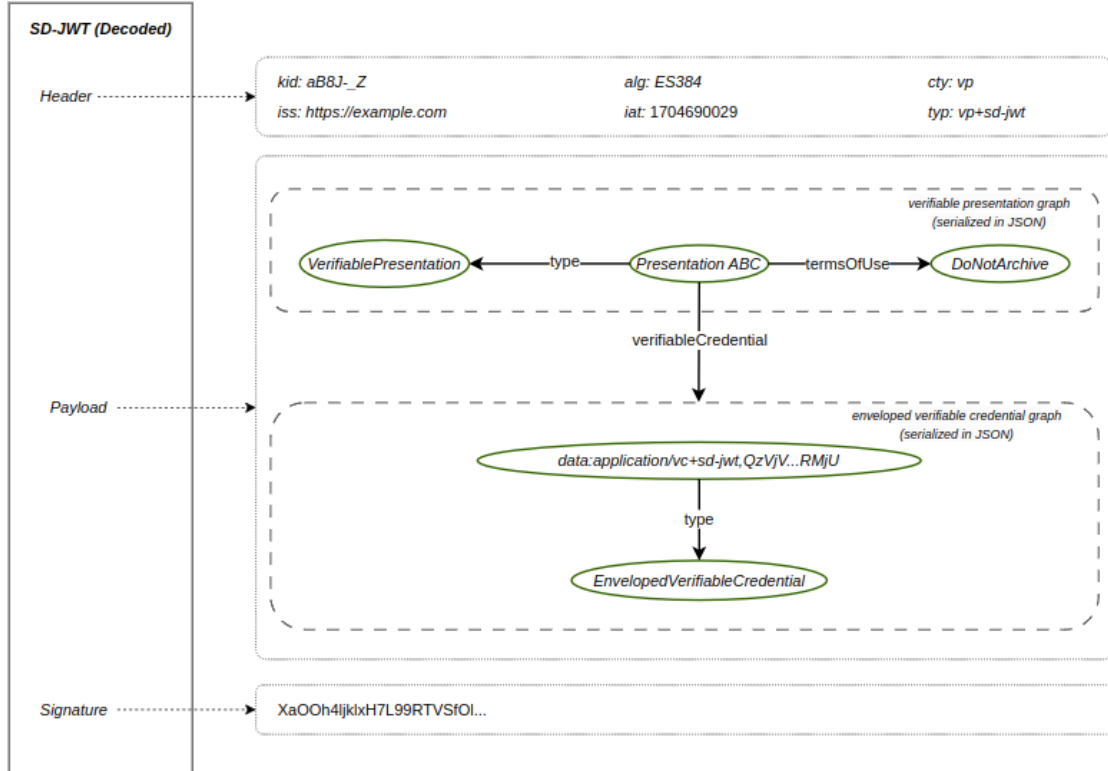


Figure A3: VCs JOSE Enveloping

- **Zero-knowledge Proof mechanism**

Zero-knowledge proof mechanism is a cryptographic way of enabling a prover to demonstrate possession of certain information such as an attribute or credential without revealing the actual data itself. In the VC, Zero-Knowledge Proofs (ZKPs) allow a credential holder to prove the validity of specific claims like instances where age is a requirement, without disclosing sensitive data e.g., full birth-date[139].

The verifiable credential data model supports ZKPs through cryptographic proof types such as CL signatures and BBS+ signatures [6], which are capable of enabling privacy-preserving credential presentation. These techniques enhance both data minimization and user autonomy, aligning with principles of SSI and privacy-by-design.

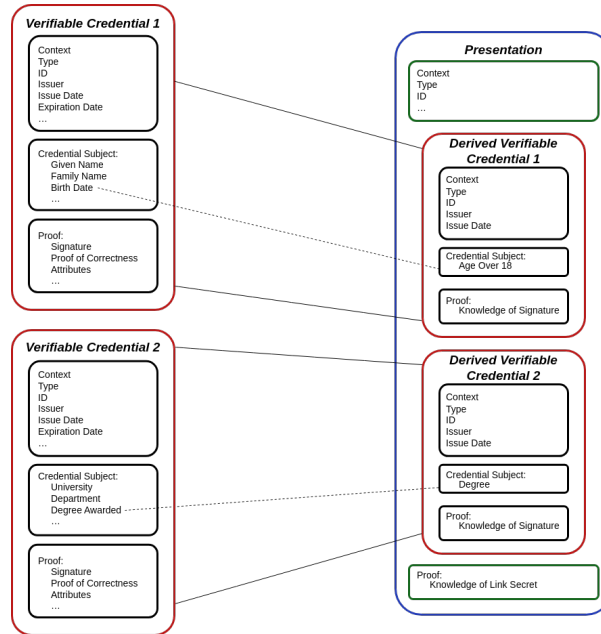


Figure A4: Selective disclosure

It has several key compatibilities as depicted in the figure above A4 with include;

- **Selective disclosure:** ZKPs enable the holder to disclose only specific claims from a credential omitting other associated data. For instance, an individual may prove eligibility for employment possessing a degree or certification without revealing personal identifiers or unrelated qualifications. This flexibility allows holders to generate derived verifiable credentials that conform with the verifiers schema, without re-engaging the issuer.
- **Unlinkable Credential presentation** Through using cryptographic techniques such as blinded signatures or ZKPs of signature possession, the holder can present credentials multiple times without enabling verifiers to correlate presentations. This unlinkability significantly reduces the risk of cross-session surveillance or identity proofing, ensuring a higher degree of anonymity and pseudonymity.
- **Non-Correlatable Subject Identification:** ZKPs also support non-correlatable identification enabling holders or subjects to prove that a credential was issued to or about them, without exposing a globally unique identifier e.g., a DID or National ID. This further enhances privacy by allowing for the combination of credentials from multiple issuers into a single presentation without disclosing identifying metadata or inter-credential links to the verifier[139].

Web3 is about grabbing some of the power back, VCs play a pivotal role by enabling individuals to take control of their digital identities unlike the previous credentials managed by centralized or federated authorities, they allow users to prove claims without intermediaries. VCs operate through key roles that facilitate its life-cycle as explained in the section 4.4.3.

In this employment verification system, VCs serve as a foundational technology to streamline credential sharing and validation. For example when a job seeker (HOLDER) presents VCs attesting to their employment history or qualifications to HR

professionals(VERIFIERS).The use of cryptographic mechanisms [134] ensures that these credentials are temper-evident enabling trust in the verification process. The W3C Vc specification as distinctly categorized VS specification into two which are both useful to the project. one specification JOSE [146] that defines how to secure credentials and presentations conforming to verifiable credential data model with JSON object signing and Encryption, Selective disclosure for JWTs, allowing Vcs data model to be implemented with standards for signing and encryption that are widely adopted, the other standard is the one most talked about verifiable credential data integrity 1.0 [174] describing mechanisms for ensuring the authenticity and integrity of VCs and similar types of constrained digital documents using cryptography.

A.3 Business Analysis

A.3.1 Value Proposition

The core value proposition of the decentralized employment verification system designed in alignment with EBSI and guided by the principles of SSI.The proposed system serves as an innovative solution for cross-boarder employment credential verification within the EU, addressing the technical, legal and administrative inefficiencies inherent in existing centralized systems.It ensures compliance with the key European frameworks, including the eIDAS Regulations and GDPR [63],[40].The value proposition is examined across multiple stakeholder dimensions, articulating its comprehensive impact on individuals, employers, credential issuers, and governmental bodies.

1. **Value for individuals(credential holders)** At the core of the proposed system is the principle of data ownership and control by individuals.By integrating SSI principles and VCs, individuals retain full autonomy over their employment-related data[60].This data is securely stored in a user-controlled digital identity wallet thereby eliminating the need for dependency on third-arty intermediaries.

Furthermore, the implementation of DIDs enables individuals to present their credentials seamlessly across borders.The system’s reliance on standardized protocols guarantees that credentials are universally verifiable with any EU member state, significantly enhancing labour mobility, a crucial element of the European single market[29].privacy measures such as selective disclosure and Zero-knowledge proofs reinforce this framework, allowing individuals to reveal only essential information during credential presentation, thereby lowering the risk of personal data exposure.

2. **value for Employers and Verifiers** Employers and credential verifiers stand to benefit immensely from the automation and trust mechanisms integrated within the system.Traditional employment verification processes often entail manual validations, translations, or notarizations, leading to considerable time and cost inefficiencies[183]. In contrast, the decentralized system facilitates real-time, automated verification of employment credentials using the cryptographic proofs and a trust registry model, which enhances operational efficiency.

verifiers gan reliable access to the assessment of the origin, authenticity, and integrity of credentials without directly contacting issuers, bolstered by EBSI’s trust model that link each issuer’s legitimacy to a verifiable trust chain initiated by a recognized Trusted Accreditation Organization.Furthermore, the risk relate to employment fraud and credential forgery are mitigated through the use of private

key signatures bound to verified DIDs, validated against a decentralized trust model, thus reducing the potential fraudulent claims significantly[149].

3. value for Issuers(employers, Accreditation Bodies, Public Institutions)

The system also presents substantial advantages for credential issuers, including employers and accredited bodies, utilizing EBSI's DID framework and trust registries empowers issuers to independently manage their cryptographic keys, fostering secure and scalable credential issuance without constant oversight from root TAO. This includes capabilities for key rotation and management of multiple associated with a single DID, thereby enhancing overall security[110].

The dynamic fetching of the DID Document from EBSI registry ensure that key updates can transpire transparently, thus maintaining uninterrupted verification process. Additionally, employing standardized data models and credential schemas, tailored for employment history, job titles and contract durations, promotes interoperability across various domains and jurisdictions, facilitating trust and consistency in credential issued across different regions or sectors[52].

4. Value for Governments and Policy Makers From a governmental perspective, the system aligns with border policy objectives such as digital sovereignty, public sector modernization, and the promotion of labor mobility. The decentralized verification infrastructure allows for the seamless recognition of employment credentials across member states, thus supporting principles of mutual recognition under EU law

The resultant decrease in administrative overhead, thanks to automating credential verification processes , translates into long-term operational cost savings for public agencies while concurrently supporting anti-fraud initiatives amid cross-boarder employment and social benefits claims. The federated governance model ensures that each member state retains jurisdictional control over credential issuance and verification through designated TAOs and sub-TAOs, thus enhancing data sovereignty while promoting interoperability[55].

A.3.2 Stakeholders

The projects implementation involves a multifaceted ecosystem of stakeholders. Each stakeholder embodies unique roles and responsibilities, which are imperative for the architectural integrity and regulatory compliance of the system. These roles encompass governance, identity issuance, credential verification, and the broader adoption of the system. A comprehensive understanding of these interactions is crucial for establishing a system that is both technically robust and compliant with legislative frameworks.

1. Governance Bodies of EBSI

The European commission, in conjunction with the European Blockchain Partnership, forms the governance framework for EBSI. This consortium, which includes EU member states and associated countries, plays a pivotal role in defining the Trust Framework alongside technical standards for decentralized identity components such as like eIDAS and GDPR, which is essential for maintaining high levels of trust as defined in section 7.2.2 among participants and safeguarding user rights[11]. The governance bodies are responsible for establishing;

- **Root Trusted Accreditation Organization(TAOs)** as essential entities within the trust chain.
- **EBSI Trust Registries** that are fundamental for credential issuer's verification
- Compliance mechanisms to align the decentralized system with current legal standards, fostering an environment of accountability and transparency.

2. Trusted Accreditation Organizations (TAOs)

TAOs serve as intermediaries between EBSI governance and various domain-specific stakeholders. In the context of employment verification, TAOs might include governmental bodies such as Ministries of Labour or recognized public employment services. Their primary functions involve the accreditation of Trusted Issuers for employment-related credentials, managing the authorization and revocation process, and actively participating in EBSI's Trust Registries.

Furthermore TAOs help establish a transparent and traceable mechanism that aids different stakeholders in maintaining trust, thereby enhancing the verification process.

3. Trusted Issuers(TIs)

TIs are critical in issuing verifiable credentials pertinent to employment, covering job titles, durations of employment, and contracts etc., This category encompasses private and public employers, recruitment agencies and industry bodies. By employing secure wallet solution with walt.id, TIs can cryptographically sign credentials that will be registered for revocation and validation purposes. Key responsibilities of TIs include;

- Ensuring the authenticity and accuracy of issued credentials.
- Regularly updating cryptographic keys according to the best practices
- Participating in governance structures aimed at shaping trust policies and ensuring interoperability.

4. Credential Holders(Employees/Job Seekers)

Credential holders, who are typically employees or job seekers, are the central beneficiaries of the SSI model, as they maintain control over their personal employment credential. Utilizing digital wallets, they can selectively disclose their information to potential verifiers[61].

The responsibilities of the credential holder include managing their private keys, presenting necessary credentials during job applications, and exercising their rights under GDPR concerning consent and disclosure. The technological infrastructure supporting these actions features non-custodial wallets tailored for SSI, reinforcing both security and user autonomy.

5. Verifiers (prospective Employers, Authorities)

Verifiers in this ecosystem, which include prospective employers and public institutions, are tasked with validating verifiable presentations to ensure the authenticity of employment credentials. They leverage status registries and DID resolution services for this purpose. A practical use case involves a Danish employer verifying a foreign job seeker's credentials issued by a French employer through the EBSI framework[2].

6. Technical Enablers, Solution Provider and Framework Developers)

The success of any decentralized identity system hinges on robust technical support from wallet-as-a-service providers and Distributed Ledger Technology maintainers. Entities such as Walt.id provide the necessary infrastructure for managing DIDs, VCs and trust registries. They ensure compliance with technical standards, including the W3C credentials Data Model, which are essential for maintaining the integrity and usability of the system. Their contributions encompass the integration of credential issuance, storage, and verification functionalities while ensuring adherence to open-source protocols and regulatory compliance. The security and interoperability of these frameworks profoundly influence the system's success and sustainability within the decentralized ecosystems[2].

7. Cross-Border Institutional Partners

Cross-border institutional partners play a critical role in fostering interoperability across different jurisdictions. Their involvement is essential for managing compliance with eIDAs Trust Lists and accreditation frameworks while facilitating the onboarding of new issuer or branches within the decentralized framework.

8. End-Users of verification

Service integrators serve as the final stakeholders, embedding employment verification processes into broader services like digital onboarding and professional licensing. They may combine employment verification with other elements such as Personal Identification Data or Qualified Electronic Signatures, creating a comprehensive identification solution.

A.4 Empirical examples of the Credentials in the current employment landscape

The figure below shows a recommendation letter as a presentable document needed for verification.



Computer Science Department
Selma Lagerlöfs Vej 300,
9220 Aalborg Ø, DK
Michele Albano
Associate Professor
Work: +4522260040
mialb@cs.aau.dk

Aalborg, 20 January 2023

Object: Recommendation for Robert Ouko Otieno

To whom it may concern,

I am writing this letter in support of Robert Ouko Otieno's application for a master's degree in computer science.

I met Robert in September 2022, when he started an internship at the Department of Computer Science of Aalborg University. In that context, Robert has been contributing to the European project domOS project. Since then, he proved to be a proactive and motivated software engineer, with a broad range of interests and a good potential as senior personnel. His contributions were of high quality, and he took an active part in laying out a plan for further research activities that can be of high relevance for the project. As a last note, he is a positive person, and it is a pleasure to work with him.

I believe that Robert would be an excellent candidate for a scholarship. He has a passion for software engineering, and I would be delighted in knowing that he moved further with his learning plans within a highly ranked Computer Science Department.

I strongly recommend Robert for a scholarship.

Please do not hesitate to contact me if you require further information or clarification.

Sincerely,

Michele Albano

A handwritten signature in blue ink, appearing to read "Michele Albano".

Figure A5: An Example of an issuer recommendation letter

This represents an educational certification that is issuer in reflection to accomplishing of a course

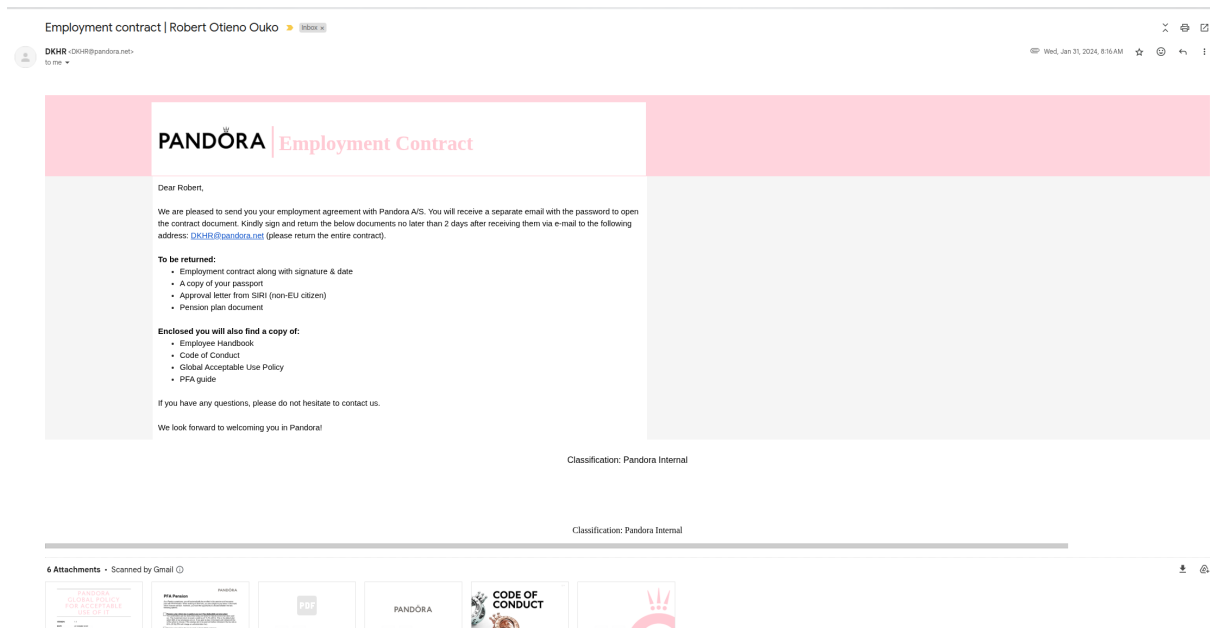


Figure A7: Requirements as proof of during employment

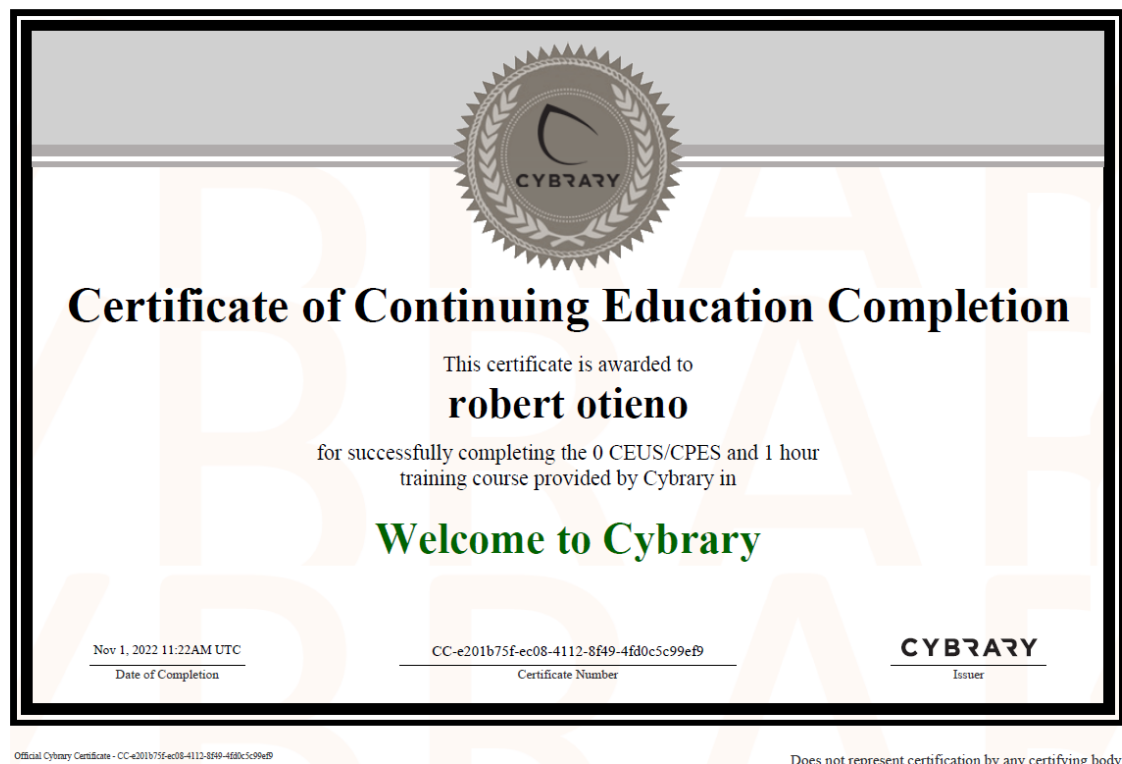


Figure A6: Certification Image verifiable in physical state

This Figure section show cases an example of requirements after interview and confirmations


```
-apt-1 : [ 22:24:31.63336489] INFO [ D-worker-3 ] : Weblog : RESP 400 -> POST http://localhost:7104/wallet-  
wallet/f5c7587f-0088-414b-bbd4-e7215c9bd844/exchange/useOffereRequest?did=didX3ajwK3AeyJrdHkOIJP5IAIcIJcnvIoIFZDNIINTE5IwaLzLKjotWtBE  
dZdaTrAYfKJWhKhNnrPRHD3OEH3I2NVUY4MUZIcwhTOTNmbyIsIngioiJBVLvdSunZONFhtQUJKSDLSxIdLVKV3WGdhZDJYQzVjNWqZ2FOURtuUtoCIno (Mozilla): body: "  
n error" (400 Bad Request)  
  
-apt-1 : [ 22:24:41.582608150] INFO [ D-worker-10 ] : Weblog : REQUEST -> GET http://localhost:7104/wallet-  
llet/f5c7587f-0088-414b-bbd4-e7215c9bd844/credentials?showDeleted=false&showPending=false (Mozilla): no body, cookies: { "login=idm79ae031  
3ca1bb8763fed341ce-2X2ZF7483ed9fa1e48152caadaceb0416f658c805ab91f8ce59069de958c5c1491e5937297bdc729dfac7C6a9806679fc863bb1ba755545e10  
e4404039eb9ab9b583598d6f8400ff7eaf3ba02d9479646f710ac74512f5aa522cd170ace65f192c457943b7e2f08d157442423b3db1ba6efd4e5eeea47b5e169d20194f3c  
fb6bdi1ef5a369y1f01b42f5dd337f12d62aba107ffe3989d60881f61814eeb6111727484a066cc33aeb6365c418c379fe1f448ba29b22f5dc325f4812eede4ebfee  
61cf125ad23c056107b6189fd42da87f5ad6ebbb41fc7410d3f13152754aaf16073396ced55072f76704dc5f14c358ec37ddb5b59911618d1f0833be6  
d26cc51f89c21dK3Aeeeb47e69485291e7a86b4a633abb1c74cf2f8b08f5448aa7eca6462287752fa, i18n_redirected=en-US, auth.token=eyJhbGciOiJIUzI1NiJ  
dMmYyOiJlbnRpdG4iZWNTenRlcTswACCIHMtMTQwMzAiNywtaWFOIjoXNDQ0ZXMDU3LCJkdGkiOiJKNjNuYWVENC5YABLRTRhZTU0ODdhMyIkzmc1MDU0Xnt0ATllCjpc3MtIOJl  
8vbG9yYmxob3N0OjcwMDELLCJhdWQiOiJodHRwOi8vbG9yYmxob3N0OjcwMDELLCJzdWIiOiI4MzQ0MmYyYjFhYi1lNDBLMWRKRnRK4ZNElFQ.1_F_dgJTGX  
AgQxiYv3eKMmBa4BMqQTbwFc")  
  
-apt-1 : [ 22:24:41.586424610] INFO [ D-worker-3 ] : Weblog : REQUEST -> GET http://localhost:7104/wallet-  
llet/f5c7587f-0088-414b-bbd4-e7215c9bd844/credentials?showDeleted=false&showPending=false (Mozilla): no body, cookies: { "login=idm79ae031  
3ca1bb8763fed341ce-2X2ZF7483ed9fa1e48152caadaceb0416f658c805ab91f8ce59069de958c5c1491e5937297bdc729dfac7C6a9806679fc863bb1ba755545e10  
e4404039eb9ab9b583598d6f8400ff7eaf3ba02d9479646f710ac74512f5aa522cd170ace65f192c457943b7e2f08d157442423b3db1ba6efd4e5eeea47b5e169d20194f3c  
fb6bdi1ef5a369y1f01b42f5dd337f12d62aba107ffe3989d60881f61814eeb6111727484a066cc33aeb6365c418c379fe1f448ba29b22f5dc325f4812eede4ebfee  
61cf125ad23c056107b6189fd42da87f5ad6ebbb41fc7410d3f13152754aaf16073396ced55072f76704dc5f14c358ec37ddb5b59911618d1f0833be6  
d26cc51f89c21dK3Aeeeb47e69485291e7a86b4a633abb1c74cf2f8b08f5448aa7eca6462287752fa, i18n_redirected=en-US, auth.token=eyJhbGciOiJIUzI1NiJ  
dMmYyOiJlbnRpdG4iZWNTenRlcTswACCIHMtMTQwMzAiNywtaWFOIjoXNDQ0ZXMDU3LCJkdGkiOiJKNjNuYWVENC5YABLRTRhZTU0ODdhMyIkzmc1MDU0Xnt0ATllCjpc3MtIOJl  
8vbG9yYmxob3N0OjcwMDELLCJhdWQiOiJodHRwOi8vbG9yYmxob3N0OjcwMDELLCJzdWIiOiI4MzQ0MmYyYjFhYi1lNDBLMWRKRnRK4ZNElFQ.1_F_dgJTGX  
AgQxiYv3eKMmBa4BMqQTbwFc")  
  
-apt-1 : [ 22:24:41.589916561] INFO [ D-worker-10 ] : Weblog : REQUEST -> GET http://localhost:7104/wallet-  
wallet/f5c7587f-0088-414b-bbd4-e7215c9bd844/credentials?showDeleted=false&showPending=false (Mozilla): body: "TextContent[application/json  
wallet": {"f5c7587f-0088-414b"} (Default)  
  
-apt-1 : [ 22:24:41.591912207] INFO [ D-worker-3 ] : Weblog : RESP DEF -> GET http://localhost:7104/wallet-  
wallet/f5c7587f-0088-414b-bbd4-e7215c9bd844/credentials?showDeleted=false&showPending=false (Mozilla): body: "TextContent[application/json  
wallet": {"f5c7587f-0088-414b"} (Default)
```

- **TEST CASE 3: A test for the verifier service was conducted**
The verifier endpoint was test and and a reponse 200 was confirm , see diagram A11

Figure A11: Verifier Service

C Appendix III

C.1 Interview Feedbacks

The meetings and interviews were held with different personal and expertise in different fields, The first meeting was based on well drafted questions prior to the meeting that it was is to document the meeting proceedings after;

C.1.1 Meeting Conversation: Insights on Employment verification Thesis Project

The meeting only had two participants; Robert (Thesis Researched) and Employee Y (Employee at pandora, HR/Compliance Expert), Dated on 16/12/2024.

The objective of the meeting was to understand the challenges, considerations, and best practices around employee verification, talent acquisition in HR processes.

The interview covered several core themes relevant to the design and implementation of a decentralized employment verification system.

- **Regional Legislation and Background Checks** Insights on this emphasized that background checks in regions like Canada are more comprehensive, often including criminal records down to the sub-district level. In contrast, Denmark relies more on referencing than invasive checks.

The relevance of this, underscore the need for the verification system o be adaptable, with region-specific configurations for background checks and data handling e.g criminal records in Canada vs referencing in Denmark.

- **Assessment and Psychometric Tools** Tools such as Korn Ferry are used to assess candidate's competences, abilities, motivations, and logical reasoning. However, the use of such assessments varies by industry.

The Relevance: The system can allow for linking public performance records with a candidate's profile, which may be voluntarily shared and verified, without depending on solely on these platforms for primary verification.

- **Reference Checks** The reference cheks often limited by legislation, typically focusing on confirming job titles ad employment dates. Any additional details are not allowed.

Relevance: This necessitates a strict adherence to privacy laws and limits the scope of the decentralized verification system to job-related facts, with additional data only being collected under explicit consent.

- **Termination and Confidentiality** Here Termination reasons are generally kept confidential, with mutual agreements being common to avoid legal conflicts.

Relevance: The system must ensure that it does not capture or disseminate termination reasons unless legally required or consented to ensure it aligns with privacy and confidentiality guidelines.

- **Sector-Specific Considerations** For high-risk sectors such as health care e.g surgeons, background checks and verification processes are more stringent.

Relevance: This reinforces the need for flexible system where certain sectors may require additional verification.

The feedback gathered from the interview aligns closely with the thesis objectives, particularly ensuring that the system can adapt to varied legal frameworks and industry needs. The insights into the regional legislative differences are especially crucial for tailoring the system to meet both privacy requirements and verification standards in different jurisdictions.

The HR employee's perspective also highlights the role of references, where their importance is diminishing in favour of more objective and verified data points

C.1.2 Meeting with People Experience Specialist

The interview covered several important themes related to post-trial employee processes, bad, split and certification verification.

- **Post-Trial Period Process** The specialist explained that after the trial period ends, employee typically transitions to permanent employment status if they meet the necessary performance metrics. If the employer is satisfied the employee is offered a formal contract, which may include benefits. If they don't the contract comes to an end.

Relevance : This emphasizes the importance of capturing the transition from temporary to permanent status in the verification. Also the importance of when to offer verifiable credentials to the employee. The system could generate a conversion credential reflecting the employee's transition based on the performance metrics and formal evaluations

- **handling Cases of Bad Splits Between the employer and the Employee** In cases where the relationship ends poorly, he mentioned that employers typically issue a separation letter. However, this is often generic to avoid legal repercussions, and rarely provides detailed reasons for termination. Employees who leave on bad terms may not have the best references, but their performance and behaviour during the trial period are still recorded.

Relevance: This underscores the need for the verification system to handle sensitive data carefully. Termination reasons should be anonymized or anonymized in case of disputes, while still allowing for the recording of key employment dates and positions. It also reinforces the need for careful data management in bad split cases, ensuring privacy protection while providing necessary employment history data.

The interview with expert provides valuable insights into the process of employment transitions, handling separations, and certification verification. Understanding these nuances is crucial for developing a robust decentralized verification framework that can accommodate various employment outcomes, including positive transitions and bad splits.

For post-trial employee periods, incorporating a "conversion" credential into the decentralized system could enhance the clarity and efficiency of the process. For cases of bad splits, the system must be designed to maintain neutrality and privacy, ensuring that sensitive details are handled appropriately.

References

- [1] “(PDF) Beyond the basic background check: hiring the “right” employees”. en. In: *ResearchGate* (Oct. 2024). DOI: [10 . 1108 / 01409171011030372](https://doi.org/10.1108/01409171011030372). URL: https://www.researchgate.net/publication/235263088_Beyond_the_basic_background_check_hiring_the_right_employees (visited on 03/27/2025).
- [2] “(PDF) Blockchain technology in the formation mechanism and strategy of brand trust in liquor e-commerce”. en. In: *ResearchGate* (). DOI: [10 . 2478 / amns . 2023 . 2 . 00827](https://doi.org/10.2478/amns.2023.2.00827). URL: https://www.researchgate.net/publication/375058205_Blockchain_technology_in_the_formation_mechanism_and_strategy_of_brand_trust_in_liquor_e-commerce (visited on 05/04/2025).
- [3] “(PDF) Verifiable Credentials: Transforming Digital Identity in the Real World”. en. In: *ResearchGate* (Mar. 2025). DOI: [10 . 32628 / CSEIT25112382](https://doi.org/10.32628/CSEIT25112382). URL: https://www.researchgate.net/publication/389725875_Verifiable_Credentials_Transforming_Digital_Identity_in_the_Real_World (visited on 04/30/2025).
- [4] *11 Must-Know Fraud Statistics for 2023 — Inscribe*. Dec. 2024. URL: <https://www.inscribe.ai/blog/11-must-know-fraud-statistics-for-2023> (visited on 02/24/2025).
- [5] *A Realist Theory of Science — Roy Bhaskar — Taylor & Francis eBooks, R*. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9780203090732/realist-theory-science-roy-bhaskar> (visited on 03/24/2025).
- [6] Masayuki Abe et al. “On the Impossibility of Structure-Preserving Deterministic Primitives”. en. In: *Theory of Cryptography*. Ed. by Yehuda Lindell. Berlin, Heidelberg: Springer, 2014, pp. 713–738. ISBN: 978-3-642-54242-8. DOI: [10 . 1007 / 978 - 3 - 642 - 54242 - 8 _ 30](https://doi.org/10.1007/978-3-642-54242-8_30).
- [7] Abdel-Jaouad Aberkane, Seppe vanden Broucke, and Geert Poels. “Toward Data Protection by Design: Assessing the Current State of GDPR Disclosure in Web Applications”. In: *2023 IEEE 31st International Requirements Engineering Conference Workshops (REW)*. ISSN: 2770-6834. Sept. 2023, pp. 218–223. DOI: [10 . 1109 / REW57809 . 2023 . 00044](https://doi.org/10.1109/REW57809.2023.00044). URL: <https://ieeexplore.ieee.org/abstract/document/10260855> (visited on 05/03/2025).
- [8] Atta Addo. “Orchestrating a digital platform ecosystem to address societal challenges: A robust action perspective”. EN. In: *Journal of Information Technology* 37.4 (Dec. 2022). Publisher: SAGE Publications Ltd, pp. 359–386. ISSN: 0268-3962. DOI: [10 . 1177 / 02683962221088333](https://doi.org/10.1177/02683962221088333). URL: <https://doi.org/10.1177/02683962221088333> (visited on 05/05/2025).
- [9] Salah T. Alshammari and Khalid Alsubhi. “Building a Reputation Attack Detector for Effective Trust Evaluation in a Cloud Services Environment”. en. In: *Applied Sciences* 11.18 (Jan. 2021), p. 8496. ISSN: 2076-3417. DOI: [10 . 3390 / app11188496](https://doi.org/10.3390/app11188496). URL: <https://www.mdpi.com/2076-3417/11/18/8496> (visited on 04/30/2025).
- [10] John Oko Ameh and Camilus Ebuka Chukwujekwu. “Employers’ Demand for Built Environment Professionals’ Employability Skills in Nigeria: Content Analysis of Job Advertisements”. en. In: *International Journal of Real Estate Studies* 14.1 (June 2020). Number: 1, pp. 28–37. ISSN: 2231-7643. DOI: [10 . 1113 / intrest . v14n1 . 133](https://doi.org/10.1113/intrest.v14n1.133). URL: <https://intrest.utm.my/index.php/intrest/article/view/133> (visited on 04/28/2025).

- [11] Jozef Andraško and Matúš Mesarčík. “Those Who Shall Be Identified: The Data Protection Aspects of the Legal Framework for Electronic Identification in the European Union”. en. In: *TalTech Journal of European Studies* 11.2 (Sept. 2021), pp. 3–24. ISSN: 2674-4619. DOI: [10 . 2478 / bjes - 2021 - 0012](https://doi.org/10.2478/bjes-2021-0012). URL: <https://www.sciendo.com/article/10.2478/bjes-2021-0012> (visited on 05/04/2025).
- [12] Eva O. Arceo-Gomez and Raymundo M. Campos-Vazquez. “Double Discrimination: Is Discrimination in Job Ads Accompanied by Discrimination in Callbacks?” en. In: *Journal of Economics, Race, and Policy* 2.4 (Dec. 2019), pp. 257–268. ISSN: 2520-842X. DOI: [10.1007/s41996-019-00031-3](https://doi.org/10.1007/s41996-019-00031-3). URL: <https://doi.org/10.1007/s41996-019-00031-3> (visited on 04/28/2025).
- [13] *Architecture and reference framework - EUDI Wallet*. URL: <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/> (visited on 05/13/2025).
- [14] Elçi Atilla. *Theory and Practice of Cryptography Solutions for Secure Information Systems*. en. Google-Books-ID: fdOeBQAAQBAJ. IGI Global, May 2013. ISBN: 9781466640313.
- [15] Adrian Bangerter, Nicolas Roulin, and Cornelius J. König. “Personnel selection as a signaling game”. In: *Journal of Applied Psychology* 97.4 (2012). Place: US Publisher: American Psychological Association, pp. 719–738. ISSN: 1939-1854. DOI: [10.1037/a0026078](https://doi.org/10.1037/a0026078).
- [16] Punam Bedi et al. “Smart Contract based Skill Verification System for Recruitment”. In: *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*. IC3-2023. New York, NY, USA: Association for Computing Machinery, Sept. 2023, pp. 147–152. ISBN: 979-8-4007-0022-4. DOI: [10 . 1145 / 3607947 . 3607973](https://doi.org/10.1145/3607947.3607973). URL: <https://doi.org/10.1145/3607947.3607973> (visited on 12/18/2024).
- [17] Rida Belahouaoui and El Houssain Attak. “Digital taxation, artificial intelligence and Tax Administration 3.0: improving tax compliance behavior – a systematic literature review using textometry (2016–2023)”. en. In: *Accounting Research Journal* 37.2 (Mar. 2024). Publisher: Emerald Publishing Limited, pp. 172–191. ISSN: 1030-9616. DOI: [10 . 1108 / ARJ - 12 - 2023 - 0372](https://doi.org/10.1108/ARJ-12-2023-0372). URL: <https://www.emerald.com/insight/content/doi/10.1108/arj-12-2023-0372/full/html> (visited on 05/01/2025).
- [18] RICHARD Bergin. “Media richness theory”. In: *Center for Homeland Defense and Security* (2016). URL: https://chds.us/coursefiles/IS4010/lectures/tech_media_richness_long/story_content/external_files/Media%20Richness%20Theory%20Script.pdf (visited on 03/17/2025).
- [19] Preeti Bhaskar, Chandan Kumar Tiwari, and Amit Joshi. “Blockchain in education management: present and future applications”. en. In: *Interactive Technology and Smart Education* 18.1 (Nov. 2020). Publisher: Emerald Publishing Limited, pp. 1–17. ISSN: 1741-5659. DOI: [10 . 1108 / ITSE - 07 - 2020 - 0102](https://doi.org/10.1108/ITSE-07-2020-0102). URL: <https://www.emerald.com/insight/content/doi/10.1108/itse-07-2020-0102/full/html> (visited on 05/10/2025).
- [20] Priti P. Bokariya and Dilip Motwani. “Decentralization of Credential Verification System using Blockchain”. In: *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 10.11 (2021). URL: <https://www.academia.edu/download/82659128/K951409101121.pdf> (visited on 11/05/2024).

- [21] James A. Breaugh. “Employee recruitment: Current knowledge and important areas for future research”. In: *Human Resource Management Review*. Critical Issues in Human Resource Management Theory and Research 18.3 (Sept. 2008), pp. 103–118. ISSN: 1053-4822. DOI: [10.1016/j.hrmr.2008.07.003](https://doi.org/10.1016/j.hrmr.2008.07.003). URL: <https://www.sciencedirect.com/science/article/pii/S1053482208000326> (visited on 03/17/2025).
- [22] Richard G. Brody. “Beyond the basic background check: hiring the “right” employees”. In: *Management Research Review* 33.3 (Jan. 2010). Ed. by James L. Bierstaker and Inshik Seol. Publisher: Emerald Group Publishing Limited, pp. 210–223. ISSN: 2040-8269. DOI: [10.1108/01409171011030372](https://doi.org/10.1108/01409171011030372). URL: <https://doi.org/10.1108/01409171011030372> (visited on 03/27/2025).
- [23] Clemens Brunner et al. “DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust”. In: *Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications*. ICBTA ’20. New York, NY, USA: Association for Computing Machinery, Mar. 2021, pp. 61–66. ISBN: 978-1-4503-8896-2. DOI: [10.1145/3446983.3446992](https://doi.org/10.1145/3446983.3446992). URL: <https://dl.acm.org/doi/10.1145/3446983.3446992> (visited on 12/02/2024).
- [24] *Build Trusted Issuer solutions — EBSI hub*. en. Mar. 2025. URL: <https://hub.ebsi.eu/get-started/build/ti> (visited on 05/13/2025).
- [25] William Burr et al. *Electronic Authentication Guideline*. en. Tech. rep. NIST Special Publication (SP) 800-63-2 (Withdrawn). National Institute of Standards and Technology, Aug. 2013. DOI: [10.6028/NIST.SP.800-63-2](https://doi.org/10.6028/NIST.SP.800-63-2). URL: <https://csrc.nist.gov/pubs/sp/800/63/2/final> (visited on 04/28/2025).
- [26] John P. Campbell and Brenton M. Wiernik. “The Modeling and Assessment of Work Performance”. en. In: *Annual Review of Organizational Psychology and Organizational Behavior* 2. Volume 2, 2015 (Apr. 2015). Publisher: Annual Reviews, pp. 47–74. ISSN: 2327-0608, 2327-0616. DOI: [10.1146/annurev-orgpsych-032414-111427](https://doi.org/10.1146/annurev-orgpsych-032414-111427). URL: <https://www.annualreviews.org/content/journals/10.1146/annurev-orgpsych-032414-111427> (visited on 01/28/2025).
- [27] Derek S. Chapman et al. “Applicant Attraction to Organizations and Job Choice: A Meta-Analytic Review of the Correlates of Recruiting Outcomes”. In: *Journal of Applied Psychology* 90.5 (2005). Place: US Publisher: American Psychological Association, pp. 928–944. ISSN: 1939-1854. DOI: [10.1037/0021-9010.90.5.928](https://doi.org/10.1037/0021-9010.90.5.928).
- [28] Michael Cheang and Georgia Lynn Yamashita. “Employers’ Expectations of University Graduates as They Transition into the Workplace”. en. In: *European Journal of Education (EJED)* 6.2 (2023). Publisher: Revistia ERIC Number: EJ1414625, pp. 22–32. ISSN: 2601-8616. URL: <https://eric.ed.gov/?id=EJ1414625> (visited on 04/28/2025).
- [29] Kang Woo Cho, Mi Hyeon Jeon, and Sang Uk Shin. “Hierarchical Sovereignty Management and Access Control based on Self-Sovereign Identity”. In: *Research Briefs on Information and Communication Technology Evolution* 7 (2021), pp. 215–221. URL: <https://rebitce.org/index.php/rebitce/article/download/131/126> (visited on 05/03/2025).
- [30] Kyle Clark, Andrew George, and Kristen Lloyd. “Trust (Your Employees), but Verify (What They Are Doing) and Keep the Verification”. en-US. In: *Home Healthcare Now* 36.2 (Apr. 2018), p. 132. ISSN: 2374-4529. DOI: [10.1097/NHH.0000000000000663](https://doi.org/10.1097/NHH.0000000000000663). URL: https://journals.lww.com/homehealthcarenurseonline/citation/2018/03000/trust__your_employees_,_but_verify__what_they_are.13.aspx (visited on 01/28/2025).

- [31] Auguste Comte. *A General View of Positivism: Or, Summary exposition of the System of Thought and Life*. en. Google-Books-ID: c1eLEAAQBAJ. DigiCat, Sept. 2022.
- [32] Brian L. Connelly et al. “Signaling Theory: A Review and Assessment”. EN. In: *Journal of Management* 37.1 (Jan. 2011). Publisher: SAGE Publications Inc, pp. 39–67. ISSN: 0149-2063. DOI: [10.1177/0149206310388419](https://doi.org/10.1177/0149206310388419). URL: <https://doi.org/10.1177/0149206310388419> (visited on 03/17/2025).
- [33] *Credentialing and Privileging - Requirements for Physician Assistants and Advanced Practice Registered Nurses — Hospital and Hospital Clinics — Medical Staff MS*. en. URL: <https://www.jointcommission.org/standards/standard-faqs/hospital-and-hospital-clinics/medical-staff-ms/000002124/> (visited on 04/28/2025).
- [34] *Credentials Community Group*. URL: <https://w3c-ccg.github.io/meetings/2022-08-22-vc-education/> (visited on 05/13/2025).
- [35] Špela Čučko and Muhamed Turkanović. “Decentralized and Self-Sovereign Identity: Systematic Mapping Study”. In: *IEEE Access* 9 (2021), pp. 139009–139027. ISSN: 2169-3536. DOI: [10.1109/ACCESS.2021.3117588](https://ieeexplore.ieee.org/abstract/document/9558805). URL: <https://ieeexplore.ieee.org/abstract/document/9558805> (visited on 04/30/2025).
- [36] *Data Verification Methodology to Facilitate Employment Database Updates for Transportation Planning - Eric Kramer, Hyunsoo Noh, Xiao Li, 2022*. URL: <https://journals.sagepub.com/doi/abs/10.1177/03611981221090243> (visited on 05/10/2025).
- [37] Matthew Davie et al. “The Trust over IP Stack”. In: *IEEE Communications Standards Magazine* 3.4 (Dec. 2019), pp. 46–51. ISSN: 2471-2833. DOI: [10.1109/MCOMSTD.001.1900029](https://ieeexplore.ieee.org/abstract/document/9031548). URL: <https://ieeexplore.ieee.org/abstract/document/9031548> (visited on 05/05/2025).
- [38] *Decentralized Identifiers (DIDs) v1.0*. URL: <https://www.w3.org/TR/did-1.0/> (visited on 04/24/2025).
- [39] *Deepfake job candidates flagged as growing cyberthreat — CFO Dive*. en-US. URL: <https://www.cfodive.com/news/deepfake-job-candidates-flagged-growing-cyberthreat-ai/745362/> (visited on 05/19/2025).
- [40] *Designing privacy-friendly data repositories: a framework...* - Google Scholar. URL: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Designing+privacy-friendly+data+repositories%3A+a+framework+for+a+blockchain+that+follows+the+GDPR&btnG= (visited on 05/03/2025).
- [41] *DID Method for Natural Persons — EBSI hub*. en. July 2024. URL: <https://hub.ebsi.eu/vc-framework/did/natural-person> (visited on 05/13/2025).
- [42] *Digital identity models: What’s next for secure and seamless travel?* en. May 2023. URL: <https://www.weforum.org/stories/2023/05/emerging-digital-identity-models-secure-and-seamless-travel/> (visited on 04/28/2025).
- [43] *Digital Identity: Leveraging the SSI Concept to Build Trust*. en. Report/Study. URL: <https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust> (visited on 11/21/2024).
- [44] *Digitising the European system for university accreditation*. en-US. URL: <https://walt.id/case-studies/eqar> (visited on 05/08/2025).

- [45] Robert L. Dipboye, Therese Macan, and Comila Shahani-Denning. “The Selection Interview from the Interviewer and Applicant Perspectives: Can’t Have One without the Other”. en. In: ed. by Neal Schmitt. Book Title: The Oxford Handbook of Personnel Assessment and Selection Edition: 1. Oxford University Press, Nov. 2012, pp. 323–352. ISBN: 978-0-19-973257-9 978-0-19-994074-5. DOI: [10 . 1093 / oxfordhb / 9780199732579 . 013 . 0015](https://doi.org/10.1093/oxfordhb/9780199732579.013.0015). URL: <https://academic.oup.com/edited-volume/28202/chapter/213175185> (visited on 03/27/2025).
- [46] Akanksha Dixit, Max Smith-Creasey, and Muttukrishnan Rajarajan. “A Decentralized IIoT Identity Framework based on Self-Sovereign Identity using Blockchain”. In: *2022 IEEE 47th Conference on Local Computer Networks (LCN)*. ISSN: 0742-1303. Sept. 2022, pp. 335–338. DOI: [10.1109/LCN53696.2022.9843700](https://doi.org/10.1109/LCN53696.2022.9843700). URL: <https://ieeexplore.ieee.org/abstract/document/9843700> (visited on 04/30/2025).
- [47] Massimo Durante. “The Online Construction of Personal Identity Through Trust and Privacy”. en. In: *Information 2.4* (Dec. 2011), pp. 594–620. ISSN: 2078-2489. DOI: [10 . 3390 / info2040594](https://doi.org/10.3390/info2040594). URL: <https://www.mdpi.com/2078-2489/2/4/594> (visited on 11/05/2024).
- [48] *EBSI and walt.id*. en-US. URL: <https://walt.id/ecosystem/ebsi> (visited on 05/13/2025).
- [49] *eIDAS Regulation — Shaping Europe’s digital future*. en. URL: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation> (visited on 11/17/2024).
- [50] *Electronic Identity Credential Trust Elevation Framework Version 1.0*. URL: <https://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csprd01/trust-el-framework-v1.0-csprd01.html> (visited on 04/28/2025).
- [51] Miriam Eliav-Feldon. “Paperwork: Identification Documents”. en. In: *Renaissance Impostors and Proofs of Identity*. Ed. by Miriam Eliav-Feldon. London: Palgrave Macmillan UK, 2012, pp. 194–217. ISBN: 9781137291370. DOI: [10 . 1057 / 9781137291370 _ 8](https://doi.org/10.1057/9781137291370_8). URL: https://doi.org/10.1057/9781137291370_8 (visited on 11/05/2024).
- [52] Nehal Ettaloui, Sara Arezki, and Taoufiq Gadi. “An Overview of Blockchain-Based Electronic Health Record and Compliance with GDPR and HIPAA”. en. In: *Artificial Intelligence, Data Science and Applications*. Ed. by Yousef Farhaoui et al. Cham: Springer Nature Switzerland, 2024, pp. 405–412. ISBN: 978-3-031-48573-2. DOI: [10.1007/978-3-031-48573-2_58](https://doi.org/10.1007/978-3-031-48573-2_58).
- [53] *EUDI Wallet and eIDAS 2: A complete guide to understanding QEAA and PID digital credentials for individuals and organizations*. en. URL: <https://www.talao.io/blog/eudi-wallet-understanding-credentials-in-eidas-2-eaa-qeaa-and-pid/> (visited on 05/13/2025).
- [54] *European Blockchain Services Infrastructure — Shaping Europe’s digital future*. en. URL: <https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure> (visited on 04/28/2025).
- [55] Benedict Faber et al. “BPDIMS: A Blockchain-based Personal Data and Identity Management System”. English. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences (HICSS), 2019, pp. 6855–6864. URL: <https://research.cbs.dk/en/publications/bpdims-a-blockchain-based-personal-data-and-identity-management-s> (visited on 05/04/2025).

- [56] Oriol Farràs, Josep Domingo-Ferrer, and Alberto Blanco-Justicia. “Privacy-Preserving Trust Management Mechanisms from Private Matching Schemes”. en. In: *Data Privacy Management and Autonomous Spontaneous Security*. Ed. by Joaquin Garcia-Alfaro et al. Berlin, Heidelberg: Springer, 2014, pp. 390–398. ISBN: 9783642545689. DOI: [10.1007/978-3-642-54568-9_26](https://doi.org/10.1007/978-3-642-54568-9_26).
- [57] *Federation of State Medical Boards*. URL: <https://www.fsmb.org/> (visited on 04/28/2025).
- [58] Anna Felkner and Adam Kozakiewicz. “RTT+-time validity constraints in RTT language”. In: *Journal of Telecommunications and Information Technology* (2012), pp. 74–82. URL: <https://yadda.icm.edu.pl/baztech/element/bwmeta1.element/baztech-article-BATA-0016-0009> (visited on 04/30/2025).
- [59] Roberta Fenech, Priya Baguant, and Dan Ivanov. “The changing role of human resource management in an era of digital transformation”. In: *International Journal of Entrepreneurship* 22.2 (2019), pp. 166–175. URL: <https://www.academia.edu/download/78857024/The-changing-role-of-human-resource-management-in-an-era-of-digital-transformation-23-1.pdf> (visited on 11/05/2024).
- [60] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. “In Search of Self-Sovereign Identity Leveraging Blockchain Technology”. In: *IEEE Access* 7 (2019), pp. 103059–103079. ISSN: 2169-3536. DOI: [10.1109/ACCESS.2019.2931173](https://doi.org/10.1109/ACCESS.2019.2931173). URL: <https://ieeexplore.ieee.org/abstract/document/8776589> (visited on 05/03/2025).
- [61] Luca Ferri et al. “Ascertaining auditors’ intentions to use blockchain technology: evidence from the Big 4 accountancy firms in Italy”. en. In: *Meditari Accountancy Research* 29.5 (Nov. 2020). Publisher: Emerald Publishing Limited, pp. 1063–1087. ISSN: 2049-372X. DOI: [10.1108/MEDAR-03-2020-0829](https://doi.org/10.1108/MEDAR-03-2020-0829). URL: <https://www.emerald.com/insight/content/doi/10.1108/medar-03-2020-0829/full/html> (visited on 05/04/2025).
- [62] M. Jayne Fleener. *Blockchain Technologies: A Study of the Future of Education*. — EBSCOhost. en. ISSN: 2158-3595 Issue: 1 Pages: 26 Volume: 22. Jan. 2022. DOI: [10.33423/jhetc.v22i1.4956](https://doi.org/10.33423/jhetc.v22i1.4956). URL: <https://openurl.ebsco.com/contentitem/doi:10.33423%2Fjhetc.v22i1.4956?sid=ebsco:plink:crawler&id=ebsco:doi:10.33423%2Fjhetc.v22i1.4956> (visited on 05/03/2025).
- [63] Marcu Florea and Beatriz Esteves. “Is Automated Consent in Solid GDPR-Compliant? An Approach for Obtaining Valid Consent with the Solid Protocol”. en. In: *Information* 14.12 (Dec. 2023). Number: 12 Publisher: Multidisciplinary Digital Publishing Institute, p. 631. ISSN: 2078-2489. DOI: [10.3390/info14120631](https://doi.org/10.3390/info14120631). URL: <https://www.mdpi.com/2078-2489/14/12/631> (visited on 05/03/2025).
- [64] Helena Francke. “Trust in the academy: a conceptual framework for understanding trust on academic web profiles”. en. In: *Journal of Documentation* 78.7 (Sept. 2021). Publisher: Emerald Publishing Limited, pp. 192–210. ISSN: 0022-0418. DOI: [10.1108/JD-01-2021-0010](https://doi.org/10.1108/JD-01-2021-0010). URL: <https://www.emerald.com/insight/content/doi/10.1108/jd-01-2021-0010/full/html> (visited on 05/01/2025).
- [65] A. Fraser and S. Schneider. “On the role of blockchain for self-sovereign identity”. In: *Competitive Advantage in the Digital Economy (CADE 2022)*. Vol. 2022. June 2022, pp. 17–21. DOI: [10.1049/icp.2022.2032](https://doi.org/10.1049/icp.2022.2032). URL: <https://ieeexplore.ieee.org/abstract/document/9945913> (visited on 04/30/2025).

- [66] *Frontiers — Health Passport: A blockchain-based PHR-integrated self-sovereign identity system*. URL: <https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2023.1075083/full> (visited on 05/05/2025).
- [67] Yunfei Ge, Tao Li, and Quanyan Zhu. “Scenario-Agnostic Zero-Trust Defense with Explainable Threshold Policy: A Meta-Learning Approach”. In: *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. ISSN: 2833-0587. May 2023, pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS57453.2023.10225816. URL: <https://ieeexplore.ieee.org/abstract/document/10225816> (visited on 04/30/2025).
- [68] Mr Nikhil Ghadge. “Digital Identity in the Age of Cybersecurity: Challenges and Solutions”. en. In: *London Journal of Research In Computer Science and Technology* 24.1 (June 2024), pp. 1–10. ISSN: 2514-8648. URL: <https://journalspress.uk/index.php/LJRCST/article/view/1023> (visited on 03/27/2025).
- [69] Maren Gierlich-Joas, Abayomi Baiyere, and Thomas Hess. “Inverse Transparency and the Quest for Empowerment Through the Design of Digital Workplace Technologies”. English. In: *Journal of the Association for Information Systems* 25.5 (2024). Publisher: Association for Information Systems, pp. 1212–1239. ISSN: 1558-3457. DOI: 10.17705/1jais.00879. URL: <https://research.cbs.dk/en/publications/inverse-transparency-and-the-quest-for-empowerment-through-the-de> (visited on 12/18/2024).
- [70] *Global strategy on human resources for health: Workforce 2030*. en. URL: <https://www.who.int/publications/i/item/9789241511131> (visited on 04/28/2025).
- [71] Alan Goode. “Digital identity: solving the problem of trust”. In: *Biometric Technology Today* 2019.10 (Dec. 2019), pp. 5–8. ISSN: 0969-4765. DOI: 10.1016/S0969-4765(19)30142-0. URL: [https://www.magonlinelibrary.com/doi/abs/10.1016/S0969-4765\(19\)30142-0](https://www.magonlinelibrary.com/doi/abs/10.1016/S0969-4765(19)30142-0) (visited on 11/05/2024).
- [72] Evan Gordenker. *False Face: Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation*. en-US. Apr. 2025. URL: <https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/> (visited on 05/19/2025).
- [73] Kimberly Seung Goulart, Jorge Rodríguez Menés, and Josep Maria Caroz Armayones. *Job descriptions, from conception to recruitment: A qualitative review of hiring practices*. eng. Working Paper 2022/06. JRC Working Papers Series on Labour, Education and Technology, 2022. URL: <https://www.econstor.eu/handle/10419/266549> (visited on 12/03/2024).
- [74] Paul A. Grassi et al. “Digital Identity Guidelines: Authentication and Lifecycle Management [includes updates as of 03-02-2020]”. en. In: *NIST* (Mar. 2020). Last Modified: 2021-10-12T11:10-04:00 Publisher: Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray Perlner, Andrew Regenscheid, William E. Burr, Justin P. Richer, Naomi Lefkowitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, Mary Theofanos. URL: <https://www.nist.gov/publications/digital-identity-guidelines-authentication-and-lifecycle-management-includes-updates-03> (visited on 04/28/2025).

- [75] Shirley Gregor and Alan R. Hevner. "Positioning and Presenting Design Science Research for Maximum Impact". In: *MIS Quarterly* 37.2 (2013). Publisher: Management Information Systems Research Center, University of Minnesota, pp. 337–355. ISSN: 0276-7783. URL: <https://www.jstor.org/stable/43825912> (visited on 03/24/2025).
- [76] *Guidance on Digital ID*. URL: <https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html> (visited on 04/28/2025).
- [77] Tamara Gutfleisch and Robin Samuel. "Hiring in border regions: experimental and qualitative evidence from a recruiter survey in Luxembourg". en. In: *Journal for Labour Market Research* 56.1 (Nov. 2022), p. 21. ISSN: 2510-5027. DOI: 10.1186/s12651-022-00327-2. URL: <https://doi.org/10.1186/s12651-022-00327-2> (visited on 04/30/2025).
- [78] Daniel Toshio Harrell et al. "Technical Design and Development of A Self-Sovereign Identity Management Platform for Patient-Centric Health Care Using Blockchain Technology". In: *Blockchain in Healthcare Today* 5 (Apr. 2022), 10.30953/bhty.v5.196. ISSN: 2573-8240. DOI: 10.30953/bhty.v5.196. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9907400/> (visited on 05/05/2025).
- [79] Bill Haskins. "Implementing a Structured Verification Framework to Improve Verification Requirements Quality". en. In: *INCOSE International Symposium* 26.1 (2016). eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/j.2334-5837.2016.00199.x>, pp. 877–891. ISSN: 2334-5837. DOI: 10.1002/j.2334-5837.2016.00199.x. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2016.00199.x> (visited on 05/04/2025).
- [80] Alan R. Hevner et al. "Design Science in Information Systems Research". In: *MIS Quarterly* 28.1 (2004). Publisher: Management Information Systems Research Center, University of Minnesota, pp. 75–105. ISSN: 0276-7783. DOI: 10.2307/25148625. URL: <https://www.jstor.org/stable/25148625> (visited on 03/24/2025).
- [81] Luc Manh Hien et al. "Determinants influencing the intention to switch internet service providers of consumers: Application of transaction costs theory". In: *Corporate Governance and Organizational Behavior Review* 6.3 (2022), pp. 56–66. URL: <https://pdfs.semanticscholar.org/4618/add87b665d131a01ed8348df02844e0c3f35.pdf> (visited on 04/30/2025).
- [82] *Hiring Process Steps for 2022*. en-US. Aug. 2018. URL: <https://www.smartrecruiters.com/resources/glossary/hiring-process-steps/> (visited on 11/19/2024).
- [83] *Impact of CV fraud on UK businesses: Employers need to know*. en-GB. June 2024. URL: <https://www.thehrdirector.com/business-news/business/impact-cv-fraud-uk-businesses-employers-need-know/> (visited on 01/28/2025).
- [84] *Innovations in RegTech*. en-US. URL: <https://www.financierworldwide.com/innovations-in-regtech> (visited on 04/28/2025).
- [85] Internal Audit Department, University Of Central Asia, Bishkek - Kyrgyzstan et al. "Leveraging Internal Audit and Blockchain to Mitigate Academic Fraud and Enhance Institutional Sustainability: A General Strain Theory Perspective". en. In: *International Journal of Social Science and Human Research* 08.01 (Jan. 2025). ISSN: 26440679, 26440695. DOI: 10.47191/ijsshr/v8-i1-59. URL: <https://www.ijsshr.in/v8i1/59.php> (visited on 05/03/2025).

- [86] *Internet Corporation for Assigned Names and Numbers (ICANN)*. URL: <https://www.icann.org/> (visited on 11/19/2024).
- [87] *Internet Crime Complaint Center (IC3) — Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions*. URL: <https://www.ic3.gov/PSA/2022/PSA220628> (visited on 05/19/2025).
- [88] *Introduction to Digital Identity*. en-US. URL: <https://walt.id/white-paper/digital-identity> (visited on 12/18/2024).
- [89] *Issue Verifiable Credentials using OpenID4VC*. en. Jan. 2024. URL: <https://curity.io/resources/learn/verifiable-credentials-issuance/> (visited on 05/06/2025).
- [90] Samta Jain, Smita Kashiramka, and P. K. Jain. “Cross-border M&As: integration practices from emerging economies”. en. In: *Journal of Business Strategy* 41.3 (Aug. 2019), pp. 21–33. ISSN: 0275-6668. DOI: [10.1108/JBS-01-2019-0018](https://doi.org/10.1108/JBS-01-2019-0018). URL: <https://www.emerald.com/insight/content/doi/10.1108/jbs-01-2019-0018/full/html> (visited on 04/30/2025).
- [91] Faton Kabashi et al. *Trustworthy Verification of Academic Credentials through Blockchain Technology*. — *EBSCOhost*. en. ISSN: 2626-8493 Issue: 9 Pages: 51 Volume: 20. Aug. 2024. DOI: [10.3991/ijoe.v20i09.48999](https://doi.org/10.3991/ijoe.v20i09.48999). URL: <https://openurl.ebsco.com/contentitem/doi:10.3991%2Fijoe.v20i09.48999?sid=ebsco:plink:crawler&id=ebsco:doi:10.3991%2Fijoe.v20i09.48999> (visited on 05/03/2025).
- [92] Meng Kang and Victoria Lemieux. “A Decentralized Identity-Based Blockchain Solution for Privacy-Preserving Licensing of Individual-Controlled Data to Prevent Unauthorized Secondary Data Usage”. en. In: *Ledger* 6 (Nov. 2021). ISSN: 2379-5980. DOI: [10.5195/ledger.2021.239](https://doi.org/10.5195/ledger.2021.239). URL: <https://ledger.pitt.edu/ojs/ledger/article/view/239> (visited on 05/08/2025).
- [93] Ioanna Angeliki Kapetanidou, Christos-Alexandros Sarros, and Vassilis Tsaoussidis. “Reputation-Based Trust Approaches in Named Data Networking”. en. In: *Future Internet* 11.11 (Nov. 2019), p. 241. ISSN: 1999-5903. DOI: [10.3390/fi11110241](https://doi.org/10.3390/fi11110241). URL: <https://www.mdpi.com/1999-5903/11/11/241> (visited on 04/30/2025).
- [94] Matt Kapko. *The North Korea worker problem is bigger than you think*. en-US. Mar. 2025. URL: <https://cyberscoop.com/north-korea-technical-workers-full-time-jobs/> (visited on 04/28/2025).
- [95] Dimitar Karadzhov et al. “More than just an add-on: enhancing discipline-specific employability skills and awareness via the virtual learning environment”. en. In: *Journal of Perspectives in Applied Academic Practice* 12.1 (Apr. 2024). Number: 1 Publisher: Edinburgh Napier University, pp. 19–35. ISSN: 2051-9788. DOI: [10.56433/jpaap.v12i1.568](https://doi.org/10.56433/jpaap.v12i1.568). URL: <https://eprints.gla.ac.uk/317749/> (visited on 04/28/2025).
- [96] Mikko Ketokivi and Saku Mantere. “Two Strategies for Inductive Reasoning in Organizational Research”. In: *Academy of Management Review* 35.2 (Apr. 2010). Publisher: Academy of Management, pp. 315–333. ISSN: 0363-7425. DOI: [10.5465/amr.35.2.zok315](https://doi.org/10.5465/amr.35.2.zok315). URL: <https://journals.aom.org/doi/abs/10.5465/amr.35.2.zok315> (visited on 03/24/2025).

- [97] Jeonghyun Kim and Putthachat Angnakoon. “Research using job advertisements: A methodological assessment”. In: *Library & Information Science Research* 38.4 (Oct. 2016), pp. 327–335. ISSN: 0740-8188. DOI: [10.1016/j.lisr.2016.11.006](https://doi.org/10.1016/j.lisr.2016.11.006). URL: <https://www.sciencedirect.com/science/article/pii/S074081881630322X> (visited on 12/03/2024).
- [98] Chalima Dimitra Nassar Kyriakidou, Athanasia Maria Papathanasiou, and George C. Polyzos. “Decentralized Identity With Applications to Security and Privacy for the Internet of Things”. en. In: *Computer Networks and Communications* (Aug. 2023), pp. 244–271. ISSN: 2972-4619. DOI: [10.37256/cnc.1220233048](https://doi.org/10.37256/cnc.1220233048). URL: <https://ojs.wiserpub.com/index.php/CNC/article/view/3048> (visited on 05/08/2025).
- [99] Mary Lacity and Erran Carmel. *Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet*. — EBSCOhost. en. ISSN: 1540-1960 Issue: 3 Pages: 241 Volume: 21. Sept. 2022. DOI: [10.17705/2msqe.00068](https://doi.org/10.17705/2msqe.00068). URL: <https://openurl.ebsco.com/contentitem/doi:10.17705%2F2msqe.00068?sid=ebsco:plink:crawler&id=ebsco:doi:10.17705%2F2msqe.00068> (visited on 12/18/2024).
- [100] Julia Levashina and Michael A. Campion. “Measuring faking in the employment interview: Development and validation of an interview faking behavior scale”. In: *Journal of Applied Psychology* 92.6 (2007). Place: US Publisher: American Psychological Association, pp. 1638–1656. ISSN: 1939-1854. DOI: [10.1037/0021-9010.92.6.1638](https://doi.org/10.1037/0021-9010.92.6.1638).
- [101] Zhiji Li. “A Verifiable Credentials System with Privacy-Preserving Based on Blockchain”. en. In: *Journal of Information Security* 13.2 (Feb. 2022). Number: 2 Publisher: Scientific Research Publishing, pp. 43–65. DOI: [10.4236/jis.2022.132003](https://doi.org/10.4236/jis.2022.132003). URL: <https://www.scirp.org/journal/paperinformation?paperid=115526> (visited on 12/18/2024).
- [102] Filip Lievens, Karen van Dam, and Neil Anderson. “Recent trends and challenges in personnel selection”. In: *Personnel Review* 31.5 (Jan. 2002). Publisher: MCB UP Ltd, pp. 580–601. ISSN: 0048-3486. DOI: [10.1108/00483480210438771](https://doi.org/10.1108/00483480210438771). URL: <https://doi.org/10.1108/00483480210438771> (visited on 03/27/2025).
- [103] Xing Liu, Bahar Farahani, and Farshad Firouzi. “Distributed Ledger Technology”. en. In: *Intelligent Internet of Things: From Device to Fog and Cloud*. Ed. by Farshad Firouzi, Krishnendu Chakrabarty, and Sani Nassif. Cham: Springer International Publishing, 2020, pp. 393–431. ISBN: 9783030303679. DOI: [10.1007/978-3-030-30367-9_8](https://doi.org/10.1007/978-3-030-30367-9_8). URL: https://doi.org/10.1007/978-3-030-30367-9_8 (visited on 11/05/2024).
- [104] JinCheng Ma and Fei Li. “Research on transaction privacy protection solutions for cross-border commerce”. en. In: *IET Blockchain* 4.S1 (2024), pp. 586–595. ISSN: 2634-1573. DOI: [10.1049/blc2.12080](https://doi.org/10.1049/blc2.12080). URL: <https://onlinelibrary.wiley.com/doi/abs/10.1049/blc2.12080> (visited on 04/30/2025).
- [105] Diksha Malhotra, Poonam Saini, and Awadhesh Kumar Singh. “How Blockchain Can Automate KYC: Systematic Review”. en. In: *Wireless Personal Communications* 122.2 (Jan. 2022), pp. 1987–2021. ISSN: 1572-834X. DOI: [10.1007/s11277-021-08977-0](https://doi.org/10.1007/s11277-021-08977-0). URL: <https://doi.org/10.1007/s11277-021-08977-0> (visited on 11/19/2024).
- [106] PETER V. MARSDEN. “The Hiring Process: Recruitment Methods”. en. In: *American Behavioral Scientist* 37.7 (June 1994). Publisher: SAGE Publications Inc, pp. 979–991. ISSN: 0002-7642. DOI: [10.1177/0002764294037007009](https://doi.org/10.1177/0002764294037007009). URL: <https://doi.org/10.1177/0002764294037007009> (visited on 12/03/2024).

- [107] Md. Mazharunnisa et al. “Blockchain In Human Resources: Ensuring Data Privacy And Transparency In Employee Management”. In: *2024 2nd International Conference on Disruptive Technologies (ICDT)*. Mar. 2024, pp. 90–95. DOI: [10 . 1109 / ICDT61202 . 2024 . 10488946](https://doi.org/10.1109/ICDT61202.2024.10488946). URL: [https : / / ieeexplore . ieee . org / abstract / document / 10488946](https://ieeexplore.ieee.org/abstract/document/10488946) (visited on 12/18/2024).
- [108] Katrin Nyman Metcalf and Ioannis F. Papageorgiou. “Increasing Trust in the Digital Market Through Regional Rules: the Case of Asia”. en. In: (Aug. 2022). Publisher: Brill. DOI: [10.1163/15718158-23020004](https://doi.org/10.1163/15718158-23020004). URL: https://brill.com/view/journals/aphu/23/2/article-p245_004.xml (visited on 03/27/2025).
- [109] *Mission critical solutions for defense and aerospace*. en-US. Jan. 2025. URL: [https : / / www . terma . com /](https://www.terma.com/) (visited on 01/27/2025).
- [110] Jayashree Mohan, Melissa Wasserman, and Vijay Chidambaram. “Analyzing GDPR Compliance Through the Lens of Privacy Policy”. en. In: *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*. Ed. by Vijay Gadepally et al. Cham: Springer International Publishing, 2019, pp. 82–95. ISBN: 978-3-030-33752-0. DOI: [10.1007/978-3-030-33752-0_6](https://doi.org/10.1007/978-3-030-33752-0_6).
- [111] Martin H Mollay et al. “Smart Hiring: Leveraging AI for Effective Employee Selection”. In: *2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI)*. Nov. 2024, pp. 1–6. DOI: [10.1109/IDICAIEI61867. 2024.10842754](https://doi.org/10.1109/IDICAIEI61867.2024.10842754). URL: <https://ieeexplore.ieee.org/abstract/document/10842754> (visited on 02/24/2025).
- [112] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. “A Conceptual Framework for Trust Models”. en. In: *Trust, Privacy and Security in Digital Business*. Ed. by Simone Fischer-Hübner, Sokratis Katsikas, and Gerald Quirchmayr. Berlin, Heidelberg: Springer, 2012, pp. 93–104. ISBN: 978-3-642-32287-7. DOI: [10.1007/978-3-642-32287-7_8](https://doi.org/10.1007/978-3-642-32287-7_8).
- [113] Alexander Mühle et al. “A survey on essential components of a self-sovereign identity”. In: *Computer Science Review* 30 (Nov. 2018), pp. 80–86. ISSN: 1574-0137. DOI: [10.1016/ j . cosrev . 2018 . 10 . 002](https://doi.org/10.1016/j.cosrev.2018.10.002). URL: <https://www.sciencedirect.com/science/article/pii/S1574013718301217> (visited on 11/21/2024).
- [114] *New digital fraud statistics in the UK and continental Europe: forced verification and deepfake cases multiply at alarming rates*. en. URL: <https://sumsub.com/newsroom/new-digital-fraud-statistics-in-the-uk-and-continental-europe-forced-verification-and-deepfake-cases-multiply-at-alarming-rates/> (visited on 02/24/2025).
- [115] *North Korea State-Sponsored Cyber Threat: Advisories — CISA*. en. URL: [https : / / www . cisa . gov / topics / cyber - threats - and - advisories / nation - state - cyber - actors / north - korea / publications](https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/north-korea/publications) (visited on 04/28/2025).
- [116] J. T. O'Donnell. *85 Percent of Job Applicants Lie on Resumes. Here's How to Spot a Dishonest Candidate*. en. Aug. 2017. URL: [https : / / www . inc . com / jt - odonnell / staggering - 85 - of - job - applicants - lying - on - resumes - .html](https://www.inc.com/jt-odonnell/staggering-85-of-job-applicants-lying-on-resumes-.html) (visited on 02/13/2025).
- [117] Ionica Oncioiu et al. “The Influence of Social Networks on the Digital Recruitment of Human Resources: An Empirical Study in the Tourism Sector”. en. In: *Sustainability* 14.6 (Jan. 2022). Number: 6 Publisher: Multidisciplinary Digital Publishing Institute, p. 3693. ISSN: 2071-1050. DOI: [10 . 3390 / su14063693](https://doi.org/10.3390/su14063693). URL: [https : / / www . mdpi . com / 2071 - 1050 / 14 / 6 / 3693](https://www.mdpi.com/2071-1050/14/6/3693) (visited on 04/28/2025).

- [118] *Overview*. en. URL: <https://docs.walt.id/community-stack/issuer/api/ecosystems/ebsi/overview> (visited on 05/13/2025).
- [119] M. Pallen. "Guide to the Internet. The world wide web". en. In: *BMJ : British Medical Journal* 311.7019 (Dec. 1995), p. 1552. DOI: [10.1136/bmj.311.7019.1552](https://doi.org/10.1136/bmj.311.7019.1552). URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC2548211/> (visited on 11/17/2024).
- [120] R. Perlman. "An overview of PKI trust models". In: *IEEE Network* 13.6 (Nov. 1999), pp. 38–43. ISSN: 1558-156X. DOI: [10.1109/65.806987](https://doi.org/10.1109/65.806987). URL: <https://ieeexplore.ieee.org/abstract/document/806987> (visited on 11/19/2024).
- [121] *PIF Report 2023: progress in legislation and increased transparency - European Commission*. en. URL: https://anti-fraud.ec.europa.eu/media-corner/news/pif-report-2023-progress-legislation-and-increased-transparency-2024-07-25_en (visited on 02/24/2025).
- [122] Kristina Potočnik et al. "Paving the way for research in recruitment and selection: recent developments, challenges and future opportunities". In: *European Journal of Work and Organizational Psychology* 30.2 (Mar. 2021). Publisher: Routledge eprint: <https://doi.org/10.1080/1359432X.2021.1904898>, pp. 159–174. ISSN: 1359-432X. DOI: [10.1080/1359432X.2021.1904898](https://doi.org/10.1080/1359432X.2021.1904898). URL: <https://doi.org/10.1080/1359432X.2021.1904898> (visited on 03/10/2025).
- [123] David C. Potter and Peter L. Ebb. "Hiring Employees: Getting the Process Right". In: *Journal of Oncology Practice* 2.5 (Sept. 2006), pp. 223–224. ISSN: 1554-7477. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2793630/> (visited on 12/03/2024).
- [124] Prasann Pradhan and Vikas Kumar. "Trust Management Models for Digital Identities". en. In: *International Journal of Virtual Communities and Social Networking (IJVCSN)* 8.4 (Oct. 2016), pp. 1–24. ISSN: 1942-9010. DOI: [10.4018/IJVCSN.2016100101](https://doi.org/10.4018/IJVCSN.2016100101). URL: <https://www.igi-global.com/article/trust-management-models-for-digital-identities/www.igi-global.com/article/trust-management-models-for-digital-identities/168625> (visited on 11/05/2024).
- [125] *Predicting Reputation in the Sharing Economy with Twitter Social Data*. URL: <https://www.mdpi.com/2076-3417/10/8/2881> (visited on 04/30/2025).
- [126] PricewaterhouseCoopers. *PwC's Global Economic Crime and Fraud Survey 2022*. en-gx. URL: <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey/2022.html> (visited on 04/28/2025).
- [127] "Privacy Protection During the Issuance and Revocation of Verifiable Credentials in Self-Sovereign Identity". en. In: *ResearchGate* (Apr. 2025). DOI: [10.1002/cpe.70084](https://doi.org/10.1002/cpe.70084). URL: https://www.researchgate.net/publication/391127829_Privacy_Protection_During_the_Issuance_and_Revocation_of_Verifiable_Credentials_in_Self-Sovereign_Identity (visited on 05/05/2025).
- [128] Agus Rahayu, M. Saparudin, and R. Hurriyati. "Factors Influencing Online Purchase Intention: The Mediating Role of Customer Trust (a Study Among University Students in Jakarta)". en. In: Atlantis Press, Feb. 2020, pp. 1–4. ISBN: 9789462528970. DOI: [10.2991/aebmr.k.200131.001](https://doi.org/10.2991/aebmr.k.200131.001). URL: <https://www.atlantis-press.com/proceedings/gcbme-18/125933732> (visited on 04/30/2025).

- [129] Sebastian Raisch and Sebastian Krakowski. “Artificial Intelligence and Management: The Automation–Augmentation Paradox”. In: *Academy of Management Review* 46.1 (Jan. 2021). Publisher: Academy of Management, pp. 192–210. ISSN: 0363-7425. DOI: [10.5465/amr.2018.0072](https://doi.org/10.5465/amr.2018.0072). URL: <https://journals.aom.org/doi/abs/10.5465/amr.2018.0072> (visited on 03/24/2025).
- [130] Aakankshu Rawat et al. *A Systematic Literature Review (SLR) On The Beginning of Resume Parsing in HR Recruitment Process & SMART Advancements in Chronological Order*. ISSN: 2693-5015. July 2021. DOI: [10.21203/rs.3.rs-570370/v1](https://doi.org/10.21203/rs.3.rs-570370/v1). URL: <https://www.researchsquare.com/article/rs-570370/v1> (visited on 04/28/2025).
- [131] *Re: info about the “did:ebasi” method from Giuseppe Tropea on 2024-07-19 (public-credentials@w3.org from July 2024)*. URL: <https://lists.w3.org/Archives/Public/public-credentials/2024Jul/0027.html> (visited on 05/13/2025).
- [132] RecordedFuture. *Despite Sanctions, North Koreans Continue to Use Foreign Technology — Recorded Future*. en. URL: <https://www.recordedfuture.com/research/north-koreans-continue-to-use-foreign-technology> (visited on 04/28/2025).
- [133] *Regulation - 910/2014 - EN - e-IDAS - EUR-Lex*. en. URL: <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng> (visited on 04/30/2025).
- [134] Maximilian Richter et al. “Cryptographic Requirements of Verifiable Credentials for Digital Identification Documents”. In: *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. ISSN: 0730-3157. June 2023, pp. 1663–1668. DOI: [10.1109/COMPSAC57700.2023.00257](https://doi.org/10.1109/COMPSAC57700.2023.00257). URL: <https://ieeexplore.ieee.org/document/10197083> (visited on 12/02/2024).
- [135] Jens Riegelsberger, M. Angela Sasse, and John D. McCarthy. “The mechanics of trust: A framework for research and design”. In: *International Journal of Human-Computer Studies* 62.3 (Mar. 2005), pp. 381–422. ISSN: 1071-5819. DOI: [10.1016/j.ijhcs.2005.01.001](https://doi.org/10.1016/j.ijhcs.2005.01.001). URL: <https://www.sciencedirect.com/science/article/pii/S1071581905000121> (visited on 11/18/2024).
- [136] sabuj. *What is the importance of Background Verification Services in Modern Hiring Strategy?* en-US. Jan. 2024. URL: <https://www.hroutsources.com/what-is-the-importance-of-background-verification-services-in-modern-hiring-strategy/> (visited on 11/05/2024).
- [137] Krzysztof Sacha. “Trust Management Languages and Complexity”. en. In: *On the Move to Meaningful Internet Systems: OTM 2011*. Ed. by Robert Meersman et al. Berlin, Heidelberg: Springer, 2011, pp. 588–604. ISBN: 9783642251061. DOI: [10.1007/978-3-642-25106-1_12](https://doi.org/10.1007/978-3-642-25106-1_12).
- [138] Hafida Saidi et al. “DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data”. In: *IEEE Access* 10 (2022), pp. 101011–101028. ISSN: 2169-3536. DOI: [10.1109/ACCESS.2022.3207803](https://doi.org/10.1109/ACCESS.2022.3207803). URL: <https://ieeexplore.ieee.org/abstract/document/9895264> (visited on 05/05/2025).
- [139] Xavier Salleras. *Citadel: Self-Sovereign Identities on Dusk Network*. arXiv:2301.09378 [cs]. Jan. 2023. DOI: [10.48550/arXiv.2301.09378](https://doi.org/10.48550/arXiv.2301.09378). URL: <http://arxiv.org/abs/2301.09378> (visited on 05/05/2025).

- [140] Rodrigo Q. Saramago et al. “A Tree-based Construction for Verifiable Diplomas with Issuer Transparency”. In: *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. Aug. 2021, pp. 101–110. DOI: [10 . 1109 / DAPPS52256 . 2021 . 00017](https://doi.org/10.1109/DAPPS52256.2021.00017). URL: <https://ieeexplore.ieee.org/abstract/document/9566198> (visited on 04/30/2025).
- [141] Prof Massimo Sargiacomo. *ECIIC 2019 10th European Conference on Intangibles and Intellectual Capital*. en. Google-Books-ID: 4tidDwAAQBAJ. Academic Conferences and publishing limited, May 2019. ISBN: 978-1-912764-19-8.
- [142] Abylay Satybaldy, Anushka Subedi, and Mariusz Nowostawski. “A Framework for Online Document Verification Using Self-Sovereign Identity Technology”. en. In: *Sensors* 22.21 (Jan. 2022), p. 8408. ISSN: 1424-8220. DOI: [10.3390/s22218408](https://doi.org/10.3390/s22218408). URL: <https://www.mdpi.com/1424-8220/22/21/8408> (visited on 04/30/2025).
- [143] Neetesh Saxena et al. “Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses”. en. In: *Electronics* 9.9 (Sept. 2020). Number: 9 Publisher: Multidisciplinary Digital Publishing Institute, p. 1460. ISSN: 2079-9292. DOI: [10.3390/electronics9091460](https://doi.org/10.3390/electronics9091460). URL: <https://www.mdpi.com/2079-9292/9/9/1460> (visited on 04/28/2025).
- [144] R. Andrew Sayer. *Method in Social Science: A Realist Approach*. en. Google-Books-ID: kr8QvOpM2RwC. Psychology Press, 1992. ISBN: 978-0-415-07607-4.
- [145] Carsten D. Schultz. “A trust framework model for situational contexts”. In: *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*. PST '06. New York, NY, USA: Association for Computing Machinery, Oct. 2006, pp. 1–7. ISBN: 9781595936042. DOI: [10 . 1145 / 1501434 . 1501494](https://doi.org/10.1145/1501434.1501494). URL: <https://doi.org/10.1145/1501434.1501494> (visited on 11/18/2024).
- [146] *Securing Verifiable Credentials using JOSE and COSE*. URL: <https://www.w3.org/TR/vc-jose-cose/> (visited on 12/02/2024).
- [147] *Self-sovereign identity*. en. Page Version ID: 1271064164. Jan. 2025. URL: https://en.wikipedia.org/w/index.php?title=Self-sovereign_identity&oldid=1271064164 (visited on 03/27/2025).
- [148] Jacopo Sesana. *The 10 principles of Self-Sovereign Identity (SSI) — Self Sovereign Identity*. it-IT. URL: <https://www.selfsovereignidentity.it/the-10-principles-of-self-sovereign-identity-ssi/> (visited on 11/21/2024).
- [149] Xiuyan Shao and Harri Oinas-Kukkonen. “How Does GDPR (General Data Protection Regulation) Affect Persuasive System Design: Design Requirements and Cost Implications”. en. In: *Persuasive Technology: Development of Persuasive and Behavior Change Support Systems*. Ed. by Harri Oinas-Kukkonen et al. Cham: Springer International Publishing, 2019, pp. 168–173. ISBN: 978-3-030-17287-9. DOI: [10.1007/978-3-030-17287-9_14](https://doi.org/10.1007/978-3-030-17287-9_14).
- [150] Irina Shapovalova and Alexander Pavlov. “Transformations in the Recruiting Services and Digitalization”. en. In: *SHS Web of Conferences* 93 (2021). Publisher: EDP Sciences, p. 04005. ISSN: 2261-2424. DOI: [10.1051/shsconf/20219304005](https://doi.org/10.1051/shsconf/20219304005). URL: https://www.shs-conferences.org/articles/shsconf/abs/2021/04/shsconf_nid2020_04005/shsconf_nid2020_04005.html (visited on 04/28/2025).

- [151] Alan Sherriff, Kaliya Young, and Michael Shea. “Editorial: Establishing Self Sovereign Identity with Blockchain”. English. In: *Frontiers in Blockchain* 5 (Aug. 2022). ISSN: 2624-7852. DOI: [10.3389/fbloc.2022.955868](https://doi.org/10.3389/fbloc.2022.955868). URL: <https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2022.955868/full> (visited on 04/30/2025).
- [152] Krishna Kumar Singh and Priyanka Srivastava. “Analysis of Factor Verification Affecting Recruitment Process Through Social Dynamics”. en. In: *Computer Networks, Big Data and IoT*. Ed. by A. Pasumpon Pandian, Xavier Fernando, and Wang Haoxiang. Singapore: Springer Nature, 2022, pp. 171–184. ISBN: 9789811908989. DOI: [10.1007/978-981-19-0898-9_13](https://doi.org/10.1007/978-981-19-0898-9_13).
- [153] SoniaLopezBravo. *X.509 certificates*. en-us. URL: <https://learn.microsoft.com/en-us/azure/iot-hub/reference-x509-certificates> (visited on 05/13/2025).
- [154] Quinten Stokkink et al. “A Truly Self-Sovereign Identity System”. In: *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. ISSN: 0742-1303. Oct. 2021, pp. 1–8. DOI: [10.1109/LCN52139.2021.9525011](https://doi.org/10.1109/LCN52139.2021.9525011). URL: <https://ieeexplore.ieee.org/abstract/document/9525011> (visited on 11/05/2024).
- [155] Dianna Stone et al. “The influence of technology on the future of Human Resource Management”. In: *Human Resource Management Review* 25 (June 2015). DOI: [10.1016/j.hrmr.2015.01.002](https://doi.org/10.1016/j.hrmr.2015.01.002).
- [156] Sujeet Raosaheb Suryawanshi, Dr Prashant B. Kumbharkar, and Dr Shailesh Kumar. “Challenges and research opportunities in self sovereign identity”. en. In: *International Journal of Advances in Electrical Engineering* 4.2 (2023). Publisher: AkiNik Publications, pp. 30–33. ISSN: 2708-4582. DOI: [10.22271/27084574.2023.v4.i2a.43](https://doi.org/10.22271/27084574.2023.v4.i2a.43). URL: <https://www.electricaltechjournal.com/archives/2023.v4.i2.A.43> (visited on 04/30/2025).
- [157] *Talent Acquisition and Recruiting Software — Workday*. en. URL: <https://www.workday.com/en-us/products/talent-management/talent-acquisition.html> (visited on 12/17/2024).
- [158] *Taleo - The future of recruiting is already here*. en. URL: <https://www.oracle.com/human-capital-management/taleo/taleo-to-oracle-recruiting/> (visited on 12/17/2024).
- [159] Evrim Tan et al. “Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy”. en. In: *Big Data and Cognitive Computing* 7.2 (June 2023). Number: 2 Publisher: Multidisciplinary Digital Publishing Institute, p. 79. ISSN: 2504-2289. DOI: [10.3390/bdcc7020079](https://doi.org/10.3390/bdcc7020079). URL: <https://www.mdpi.com/2504-2289/7/2/79> (visited on 04/30/2025).
- [160] David Temoshok et al. *Digital Identity Guidelines: Identity Proofing and Enrollment*. en. Tech. rep. NIST Special Publication (SP) 800-63A-4 (Draft). National Institute of Standards and Technology, Aug. 2024. DOI: [10.6028/NIST.SP.800-63A-4.2pd](https://doi.org/10.6028/NIST.SP.800-63A-4.2pd). URL: <https://csrc.nist.gov/pubs/sp/800/63/a/4/2pd> (visited on 04/28/2025).
- [161] Avraam Tepelidis et al. “BlockAdemiC: A Digital Distributed Verification System for Educational Activities in Higher Education”. In: *Distrib. Ledger Technol.* (Nov. 2024). Just Accepted. DOI: [10.1145/3703463](https://doi.org/10.1145/3703463). URL: <https://dl.acm.org/doi/10.1145/3703463> (visited on 04/30/2025).
- [162] *The Logic of Scientific Discovery — Karl Popper, Karl Popper — Taylor*. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9780203994627/logic-scientific-discovery-karl-popper-karl-popper> (visited on 03/24/2025).

- [163] *The Path to Self-Sovereign Identity*. en. Apr. 2016. URL: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/> (visited on 11/19/2024).
- [164] T. P. Thebe and der Waldt G. van der. “A recruitment and selection process model”. In: *Administratio Publica* 22.3 (Sept. 2014). Publisher: Association of Southern African Schools and Departments of Public Administration and Management (ASSADPAM), pp. 6–29. DOI: [10.10520/ejc-adminpub-v22-n3-a2](https://doi.org/10.10520/ejc-adminpub-v22-n3-a2). URL: <https://journals.co.za/doi/abs/10.10520/ejc-adminpub-v22-n3-a2> (visited on 03/10/2025).
- [165] Thapelo Phillip Thebe. “A comprehensive human resource recruitment and selection model : the case of the Department of Justice and Constitutional Development”. In: (Jan. 2014). URL: https://www.academia.edu/65648296/A_comprehensive_human_resource_recruitment_and_selection_model_the_case_of_the_Department_of_Justice_and_Constitutional_Development (visited on 03/10/2025).
- [166] Derek Torrington et al. *Human resource management*. Pearson UK, 2020. URL: [https://books.google.com/books?hl=en&lr=&id=9-csEAAQBAJ&oi=fnd&pg=PT24&dq=Torrington,+D.,+Hall,+L.,+Taylor,+S.,+%26+Atkinson,+C.+\(2020\).+Human+resource+management+\(11th+ed.\).+Pearson.&ots=uMRAzP3zkH&sig=D9cbZZNq1B04tirvwhUSaEphZh8](https://books.google.com/books?hl=en&lr=&id=9-csEAAQBAJ&oi=fnd&pg=PT24&dq=Torrington,+D.,+Hall,+L.,+Taylor,+S.,+%26+Atkinson,+C.+(2020).+Human+resource+management+(11th+ed.).+Pearson.&ots=uMRAzP3zkH&sig=D9cbZZNq1B04tirvwhUSaEphZh8) (visited on 03/27/2025).
- [167] Donald M. Truxillo et al. “Effects of Explanations on Applicant Reactions: A meta-analytic review”. en. In: *International Journal of Selection and Assessment* 17.4 (2009). eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-2389.2009.00478.x>, pp. 346–361. ISSN: 1468-2389. DOI: [10.1111/j.1468-2389.2009.00478.x](https://doi.org/10.1111/j.1468-2389.2009.00478.x). URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2389.2009.00478.x> (visited on 03/17/2025).
- [168] Muhamed Turkanović and Blaž Podgorelec. “Signing Blockchain Transactions Using Qualified Certificates”. In: *IEEE Internet Computing* 24.6 (Nov. 2020), pp. 37–43. ISSN: 1941-0131. DOI: [10.1109/MIC.2020.3026182](https://doi.org/10.1109/MIC.2020.3026182). URL: <https://ieeexplore.ieee.org/abstract/document/9206057> (visited on 04/30/2025).
- [169] Stephen Park Turner. “Durkheim’s The Rules of Sociological Method: Is It a Classic?” EN. In: *Sociological Perspectives* 38.1 (Mar. 1995). Publisher: SAGE Publications Inc, pp. 1–13. ISSN: 0731-1214. DOI: [10.2307/1389258](https://doi.org/10.2307/1389258). URL: <https://doi.org/10.2307/1389258> (visited on 03/24/2025).
- [170] V. R. Uma, Ilango Velchamy, and Deepika Upadhyay. “Recruitment Analytics: Hiring in the Era of Artificial Intelligence”. In: *The Adoption and Effect of Artificial Intelligence on Human Resources Management, Part A*. Ed. by Pallavi Tyagi et al. Emerald Publishing Limited, Jan. 2023, pp. 155–174. ISBN: 9781803820279 9781803820286. DOI: [10.1108/978-1-80382-027-920231008](https://doi.org/10.1108/978-1-80382-027-920231008). URL: <https://doi.org/10.1108/978-1-80382-027-920231008> (visited on 02/24/2025).
- [171] Andrea Vázquez-Ingelmo, Francisco J. García-Peñalvo, and Roberto Therón. “Taking advantage of the software product line paradigm to generate customized user interfaces for decision-making processes: a case study on university employability”. en. In: *PeerJ Computer Science* 5 (July 2019). Publisher: PeerJ Inc., e203. ISSN: 2376-5992. DOI: [10.7717/peerj-cs.203](https://doi.org/10.7717/peerj-cs.203). URL: <https://peerj.com/articles/cs-203> (visited on 04/28/2025).
- [172] *Velocity IT — Automation in HR: Revolutionising Talent Management*. en. URL: <https://www.velocity-it.com/knowledge-hub/automation-in-hr/> (visited on 11/05/2024).

- [173] *Verifiable Credential Data Integrity 1.0*. URL: <https://www.w3.org/TR/vc-data-integrity/> (visited on 12/02/2024).
- [174] *Verifiable Credentials Overview*. URL: <https://www.w3.org/TR/vc-overview/> (visited on 03/10/2025).
- [175] V.H. Vroom. *Work and motivation*. Work and motivation. Oxford, England: Wiley, 1964.
- [176] *Wallet for Issuers - EU Digital Identity Wallet -*. URL: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Wallet+for+Issuers> (visited on 05/13/2025).
- [177] webdesk. *Mandiant 2024 Cybersecurity Report: Key Insights on Global Cyber Threats and Attacks*. en-US. Apr. 2025. URL: <https://csopakistan.com/mandiant-2024-cybersecurity-report-key-insights-on-global-cyber-threats-and-attacks/> (visited on 04/28/2025).
- [178] Robert H. Welton and Laurel Moody. “CE: How to Write an Effective Résumé”. en-US. In: *AJN The American Journal of Nursing* 123.4 (Apr. 2023), p. 34. ISSN: 0002-936X. DOI: 10.1097/01.NAJ.0000925500.62874.39. URL: https://journals.lww.com/ajnonline/fulltext/2023/04000/CE_How_to_Write_an_Effective_R_sum_.25.aspx?context=LatestArticles (visited on 04/28/2025).
- [179] *What is CSAM ? - CSAM.be*. URL: <https://www.csam.be/en/about-csam.html> (visited on 11/19/2024).
- [180] Anna Wilson and Stefano De Paoli. “On the ethical and political agency of online reputation systems”. en. In: *First Monday* 24.2 (Feb. 2019). ISSN: 1396-0466. DOI: 10.5210/fm.v24i2.9393. URL: <http://dspace.stir.ac.uk/handle/1893/28675> (visited on 04/30/2025).
- [181] Candy So Suk Yi et al. “Benefits and use of blockchain technology to human resources management: a critical review”. In: *International Journal of Human Resource Studies* 10.2 (2020), pp. 131140–131140. URL: <https://pdfs.semanticscholar.org/40d9/93c6d3c772eeb23a802e3494506bf9b90733.pdf> (visited on 04/30/2025).
- [182] Yibei Yin. “Big Data Analysis and Modeling Method of College Student Employment Management Based on Deep Learning Model”. en. In: *International Journal of Web-Based Learning and Teaching Technologies (IJWLTT)* 18.2 (Feb. 2023). Publisher: IGI Global Scientific Publishing, pp. 1–15. ISSN: 1548-1093. DOI: 10.4018/IJWLTT.330245. URL: <https://www.igi-global.com/article/big-data-analysis-and-modeling-method-of-college-student-employment-management-based-on-deep-learning-model/www.igi-global.com/article/big-data-analysis-and-modeling-method-of-college-student-employment-management-based-on-deep-learning-model/330245> (visited on 05/10/2025).
- [183] Xiaoyang Zhu and Youakim Badr. “Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions”. en. In: *Sensors* 18.12 (Dec. 2018). Number: 12 Publisher: Multidisciplinary Digital Publishing Institute, p. 4215. ISSN: 1424-8220. DOI: 10.3390/s18124215. URL: <https://www.mdpi.com/1424-8220/18/12/4215> (visited on 05/04/2025).
- [184] Mircea Zloteanu et al. “Digital Identity: The effect of trust and reputation information on user judgement in the Sharing Economy”. en. In: *PLOS ONE* 13.12 (Dec. 2018), e0209071. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0209071. URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0209071> (visited on 04/30/2025).