

Univerza v Ljubljani
Fakulteta *za gradbeništvo*
in geodezijo



POLINA SHERSTOBITOVA

A SELF-SOVEREIGN DIGITAL WALLET FOR SUSTAINABLE
CONSTRUCTION

SAMOSUVERENE DIGITALNE DENARNICE ZA
TRAJNOSTNOSTNO GRADBENIŠTVO



European Master in
Building Information Modelling

Master thesis No.:

Supervisor:
Prof. Boštjan Brank, Ph.D.

Co-Supervisor:
Prof. Vlado Stankovski, Ph.D.

Ljubljana, 2023



ERRATA

Page

Line

Error

Correction

»This page is intentionally blank«

BIBLIOGRAFSKO – DOKUMENTACIJSKA STRAN IN IZVLEČEK

UDK: 004.7:69-021.131(043.3)

Avtor: Polina Sherstobitova

Mentor: prof. dr. Boštjan Brank

Somentor: prof. dr. Vlado Stankovski

Naslov: Samosuverene digitalne denarnice za trajnostno gradbeništvo

Tip dokumenta: Magistrsko delo

Obseg in oprema: 82 str, 79 sl., 12 pregl.

Ključne besede: SSI, trajnostno gradbeništvo, gradbeništvo 4.0, BIM

Izvleček:

Z uveljavljanjem Web3, Gradbeništva 4.0 in s prehodom na BIM raven 3 prihaja val inovativnih tehnologij, ki zahtevajo svež pristop k vzpostavljanju varnih povezav in varovanju občutljivih informacij. Ta premik zahteva opuščanje tradicionalnih identitet na papirju in prehod k digitalnim alternativam. V tem kontekstu se pojavi samoupravna identiteta (SSI) kot ključna rešitev. SSI posameznikom in subjektom v gradbeni industriji omogoča popoln nadzor nad njihovimi digitalnimi identitetami, zagotavljajoč zasebnost, varnost in brezhibno avtentikacijo na različnih platformah in sistemih. S prehodom na SSI se gradbeni industrija podaja na pot preobrazbe, ki pooblašča deležnike, da samozavestno krmarijo po zapletenem terenu sodobnih gradbenih procesov in tehnologij. Študija zagovarja uvedbo samoupravne denarnice, prilagojene posebej za gradbeni sektor, ki izkorišča zmožnosti decentraliziranih identifikatorjev in preverljivih poverilnic. Ta digitalna denarnica deluje kot visoko varno skladišče za vse podatke, povezane z gradnjo, zagotavljajoč tako integriteto kot dostopnost teh dragocenih informacij. Naš predlog sistema še posebej poudarja dve ključni vlogi v tem ekosistemu: izvajalce in gradbena podjetja. Vsaka preverljiva poverilnica je zapleteno povezana s svojim edinstvenim decentraliziranim identifikatorjem (DID), ki je varno shranjen v register na verigi.

»This page is intentionally blank«

BIBLIOGRAPHIC– DOCUMENTALISTIC INFORMATION AND ABSTRACT

UDC: 004.7:69-021.131(043.3)

Author: Polina Sherstobitova

Supervisor: prof. Boštjan Brank, Ph.D.

Cosupervisor: prof. Vlado Stankovski, Ph.D.

Title: A Self-Sovereign Digital Wallet for Sustainable Construction

Document type: Master Thesis

Scope and tools: 82 p., 79 fig., 12 tab.

Keywords: SSI, Sustainable Construction, Construction 4.0, BIM

Abstract:

The advent of Web3, Construction 4.0, and the transition to BIM Level 3 has ushered in a wave of innovative technologies that call for a fresh approach to establishing secure connections and safeguarding sensitive information. This shift demands a departure from traditional paper-based identity methods to embrace digital alternatives. In this context, self-sovereign identity (SSI) emerges as a pivotal solution. SSI empowers individuals and entities within the construction industry to maintain full control over their digital identities, guaranteeing privacy, security, and seamless authentication across diverse platforms and systems. Through the adoption of SSI, the construction industry embarks on a transformative journey, empowering its stakeholders to confidently navigate the intricate terrain of contemporary construction processes and technologies. This study advocates for the creation of a self-sovereign digital wallet tailored specifically for the construction sector, harnessing the capabilities of Decentralized Identifiers and Verifiable Credentials. This digital wallet serves as a highly secure repository for all building-related data, ensuring both the integrity and accessibility of this valuable information. Our system proposal places particular emphasis on two key roles within this ecosystem: Contractors and Construction Companies. Each verifiable credential is intricately linked to a unique DID, securely stored in an on-chain registry.

»This page is intentionally blank«

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude and appreciation to all those who have contributed to the completion of this dissertation. This academic journey has been both challenging and rewarding, and I couldn't have achieved this milestone without the support and encouragement of many individuals.

First and foremost, I am profoundly grateful to my supervisor, Prof. Vlado Stankovski and to the members of the project team - doc. dr. Petar Kochovski, Pouriya Miri and Arvin Jušić, whose unwavering guidance, expertise, and patience have been instrumental in shaping this research.

Also, I want to thank my beloved family. I am eternally grateful for your unconditional love and unwavering support throughout this academic endeavor.

My friends and colleagues have played a vital role in my academic journey. Our travel, gatherings and moral support have helped alleviate the pressures of this undertaking, making it more enjoyable.

Finally, I want to express my appreciation to the advisors of this research, prof. Tomo Cerovsek and Dina Jovanovic, whose involvement improved this study.

To all those mentioned above and to anyone else who has been a part of my academic pursuit, I offer my heartfelt thanks. Your encouragement, assistance, and belief in my abilities have been indispensable.

»This page is intentionally blank«

TABLE OF CONTENTS

ERRATA	II
BIBLIOGRAFSKO – DOKUMENTACIJSKA STRAN IN IZVLEČEK	IV
BIBLIOGRAPHIC– DOCUMENTALISTIC INFORMATION AND ABSTRACT.....	VI
ACKNOWLEDGEMENTS	VIII
TABLE OF CONTENTS	X
INDEX OF FIGURES	XII
INDEX OF TABLES	XVI
1 INTRODUCTION	1
1.1 Overview	1
1.2 Scope and Objective	2
2 STATE OF THE ART	3
2.1 Examination of Contemporary Trends	3
2.1.1 Sustainable Construction	3
2.1.2 Construction 4.0.....	5
2.1.3 BIM.....	7
2.1.4 A Brief Overview of Web3	10
2.2 Overview of Digital Identity.....	11
2.2.1 The Evolution of Digital Identity	12
2.2.2 Use Cases.....	17
3 TECHNOLOGY BACKGROUND: SELF-SOVEREIGN DIGITAL IDENTITY...20	
3.1 SSI Architecture	21
3.2 Verifiable Credentials.....	23
3.2.1 Claims	24
3.1 Verifiable Presentation	25
3.2 Syntactic Representations.....	25

3.3	Roles of Self-Sovereign Identity.....	26
3.4	Decentralized Identifiers.....	28
3.4.1	DID Document.....	29
3.4.2	DID Methods.....	30
3.5	Digital Wallets and Agent.....	31
4	CASE STUDY: SELF-SOVEREIGN DIGITAL WALLET FOR AEC INDUSTRY	33
4.1	SSI Data Model.....	36
4.2	Scenarios of SSI Implementation.....	38
4.2.1	Enhancing Web Services Authentication via DIDs.....	39
4.2.2	Establishing Secure Data Exchange Channels.....	41
4.3	Securing VCs, NFTs, IoT data and DIDs Storage in Digital Wallets.....	44
4.3.1	GUI of Digital Wallet	44
4.4	DIDs.....	50
4.5	Credentials	54
4.6	IFC-to-LBD.....	65
4.7	Implementation of a Digital Wallet with SwiftUI	67
5	CONCLUSION	75
5.1	Future Work.....	76
6	REFERENCES	77

INDEX OF FIGURES

Figure 1. Ineffective ID Systems.....	1
Figure 2: Survey results of public sentiment regarding these identity paradigms.....	2
Figure 3. Scope of literature review	3
Figure 4: Sustainable building profile and related information sources.....	4
Figure 5. The key components of Industry 4.0.....	6
Figure 6 Cyber vulnerabilities	7
Figure 7: IFC-to-LBD conversion process	9
Figure 8: The linked data cloud for the AEC project	10
Figure 9. Seven separate research streams	12
Figure 10: A compilation of attributes that are digitally recorded and stored for different use-cases.....	14
Figure 11: Digital identity models.....	15
Figure 12: Centralized identity model.....	15
Figure 13. Centralized identity model	16
Figure 14. Decentralized identity model	17
Figure 15: The walt.id website use cases	19
Figure 16: The three pillars of SSI	20
Figure 17: SSI data model	21
Figure 18: The SSI stack as a four-layer model	22
Figure 19: Basic components of a verifiable credential	24
Figure 20: The basic structure of a claim with various aspects of a subject	24
Figure 21: A syntactic representations of a verifiable credential	26
Figure 22: Roles of Self-Sovereign Identity.....	27
Figure 23 An example of a browser address bar displaying the URL for the web page.....	28
Figure 24: The format of DID	29
Figure 25: The major components of Decentralized Identifier architecture	29
Figure 26: Relationships between DID, DID subject and DID document	30
Figure 27: Data sharing through protected digital channels.....	33
Figure 28: SSI connection	34
Figure 29: SSDW for Sustainable Construction.....	35
Figure 30: SSI Data model for a system proposal.....	36
Figure 31: Example of visualization of data model diagrams from DBML code.....	36

Figure 32: DBML code for tables	37
Figure 33: DBML code for relationships between tables	37
Figure 34: SSI Kit integration.....	39
Figure 35. Scenario of SSI Implementation for getting access to marketplace and peer over secure channel.....	40
Figure 36: IDEF0 diagram depicting Scenario of SSI Implementation for getting access to marketplace	41
Figure 37: Scenario of SSI Implementation for Data exchange	42
Figure 38: DID with a public and private key	43
Figure 39: The PKI trust triangle includes a digital identifier for the controller	44
Figure 40: Digital wallet views map	45
Figure 41: Launch and login screens	46
Figure 42: GUI for Home View and Wallet views of the Contractor’s Wallet	47
Figure 43: GUI of “Apply for services” views	48
Figure 44: GUI for Home View and Wallet views of the Construction Company Wallet	49
Figure 45: GUI of “My services” views	49
Figure 46: A storage for various components such as VCs, DIDs, keys, and other essential data.....	51
Figure 47: Exposed endpoints.....	51
Figure 48: Creation and anchoring of a new DID on the EBSI ledger – Source: walt.id.....	51
Figure 49: DID creation	52
Figure 50:List of created DIDs	52
Figure 51: DID resolution	54
Figure 52: Template for Construction Company VC.....	57
Figure 53: Template for Building Passport VC	58
Figure 54: Template for LEED Certification VC	59
Figure 55: Template for Building Elements VC.....	60
Figure 56: Template for Contractor VC.....	61
Figure 57: Template for Licenses VC.....	62
Figure 58: Template for Licenses VC.....	63
Figure 59: Template addition with SSI Kit API	63
Figure 60: VC Templates with SSI Kit API	64
Figure 61: VC issuance with SSI Kit API.....	64
Figure 62: VC for Contractor.....	65

Figure 63: IFC-to-LBD.....	66
Figure 64 IFC-to-LBD converter start.....	66
Figure 65: IFC-to-LBD converter interface.....	67
Figure 66: JSON representation of the IFCtoLBD transfer.....	67
Figure 67: The app icon.....	68
Figure 68: The Launch Screen.....	68
Figure 69: The MainView Screen	69
Figure 70: The WalletView VCs Screen	69
Figure 71: The Detail View of VCs.....	70
Figure 72: The DIDs Screen.....	70
Figure 73: The ApplyView Screen.....	71
Figure 74: The Share Credentials Screen.	71
Figure 75: The Construction Company Main View Screen	72
Figure 76: The Construction Company VCs Screen	72
Figure 77: The Construction Company DIDs Screen.....	73
Figure 78: The “My services” screen	73
Figure 79: The Share Credentials Screen	74

»This page is intentionally blank«

INDEX OF TABLES

Table 1: DID key roles	52
Table 2: Basic DID properties	53
Table 3: Verification Method Properties	53
Table 4. Verifiable Credentials for Construction Industry	54
Table 5 Basic VC's properties.....	56
Table 6: Construction Company claims	56
Table 7: Building passport claims	57
Table 8: LEED certification claims	58
Table 9: Building elements claims	59
Table 10: Contractor Information claims	60
Table 11: Licenses claims.....	61
Table 12: Insurance claims	62

LIST OF ABBREVIATIONS

AEC	Architecture, Engineering, Construction
AI	Artificial Intelligence
API	Application Programming Interface
BIM	Building Information Modeling
BOT	Building Topology Ontology
CPPS	Cyber-Physical Production System
CPS	Cyber-Physical System
DBML	Database Markup Language
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
EBSI	European Blockchain Services Infrastructure
GUI	Graphical user interface
GUID	Globally unique identifier
ICT	Information and Communication Technology
IDEF	Integration DEFinition
IDP	Identity Providers
IFC	Industry Foundation Classes
IOT	Internet of Things
IPD	Integrated Project Delivery
JSON	JavaScript Object Notation
JWK	JSON Web Key
LBD	Linked Building Data
LD	Linked Data
LOD	Linked Open Data
NFT	Non-fungible token
OIDC	OpenID Connect
OWL	Web Ontology Language
RDF	Resource Description Framework
SBP	Sustainable Building Profile
SSDW	Self-Sovereign Digital Wallet

SSI	Self-Sovereign Identity
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VC	Verifiable Credential
VP	Verifiable Presentation

1 INTRODUCTION

1.1 Overview

One of the most crucial hurdles to achieving economic success in sustainable construction projects is effective communication and coordination among diverse disciplines within the project team. This entails collaborating on various aspects such as site selection, construction materials, techniques, building systems, subsystems, and even the commissioning and decommissioning of sustainable built assets. Traditional construction management methods, often characterized by linear and fragmented approaches, can introduce higher risks to sustainable construction projects, ultimately leading to cost inefficiencies (Goh, Su and Rowlinson, 2023).

The construction sector is undergoing a profound metamorphosis, propelled by emerging paradigms like Construction 4.0 and the escalating maturation of Building Information Modeling (BIM). Within this transformative journey, a plethora of challenges has emerged, encompassing realms such as cyber-security, digital identity management and insufficient information sharing. These issues have become major hurdles in the industry's progress and development (Teisserenc and Sepasgozar, 2022).

The challenge of managing digital identities presents a crucial and complex issue within extensive digital frameworks. The current generation of digital identity management systems is plagued by frequent data breaches, leaks, and privacy infringements. These problems often stem from the reliance on centralized trusted entities to oversee all aspects of user identities (Dhamija and Dusseault, 2008). Figure 1 illustrates the repercussions of ineffective ID systems, leading to global challenges across various domains. (Vasiliu-Feltes, Ingrid, Mysore, 2022).



Figure 1: Ineffective ID Systems - Source: (Vasiliu-Feltes, Ingrid, Mysore, 2022)

Cheqd.io conducted a survey involving 114 respondents to gauge their perspectives on the current digital identity systems and regulations in comparison to decentralized identity solutions. Figure 2 provides an insightful visual representation of the survey results, offering valuable insights into public sentiment regarding these identity paradigms.



Figure 2: Survey results of public sentiment regarding these identity paradigms- Source: Cheqd.io

This thesis is focused on the exploration a new digital identity model - Self-Sovereign Identity (SSI) in the construction industry. This concept aims to decentralize the management of digital identities. SSI offers the promise of granting users' control over the collection, storage, and sharing of their own identity data. The current solution is not efficient because it requires long administrative processes where many documents and information must be given out. In addition to making those identity management solutions easy to use for stakeholders, they also needed to be secure and respect data privacy which is why SSI appeared as the best technology.

1.2 Scope and Objective

The work proceeds in four methodological steps, i.e. milestones:

1. Exploration the use of digital identity in the emerging construction industry paradigms.
2. Exploration of the concept of the self-sovereign digital identity
3. Detailed design of the solution for construction industry
4. Implementation and demonstration: implementation of the designed wallet.

2 STATE OF THE ART

The systematic literature review method was adopted to identify journal articles, books, reports, and websites that describe and investigate the use of SSI in the emerging construction industry paradigms: Sustainable Construction, Construction 4.0, Web3, and BIM.

Initially, an extensive literature exploration was initiated through keyword-based searches utilizing databases such as Scopus, and Google Scholar. The search criteria encompassed terms like BIM, Sustainable and Smart Construction, Web3, Self-sovereign identity, and Construction 4.0. Publications containing these precise terms in their titles, abstracts, or keywords were earmarked as potential candidates. Subsequently, a more in-depth and exhaustive investigation was undertaken with the assistance of search engines, encompassing a spectrum of articles, including those from journals and conferences, along with review papers (Figure 3).

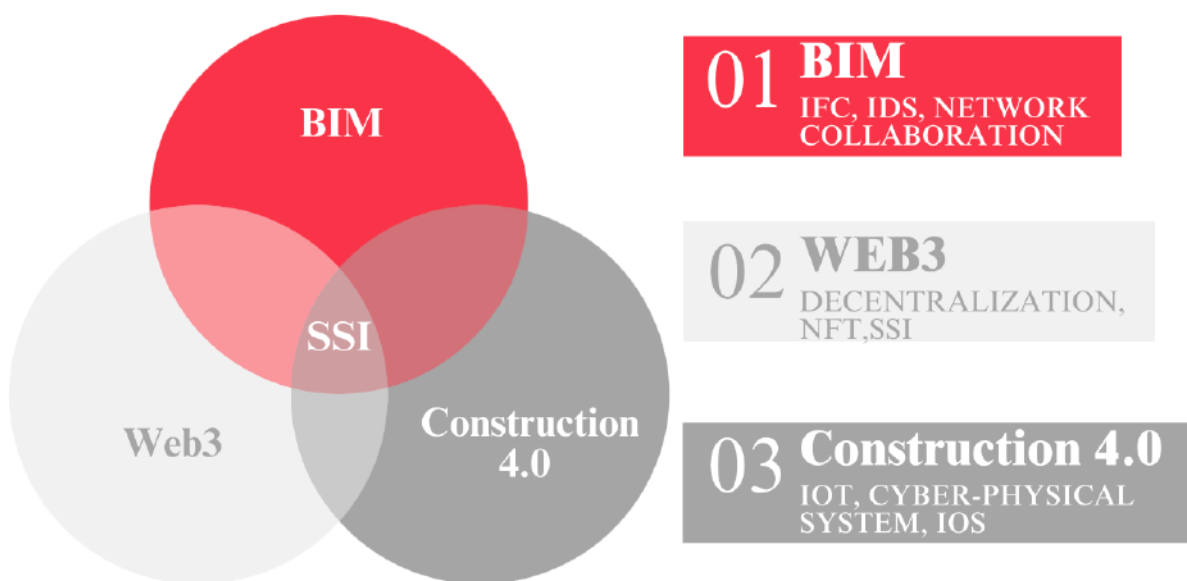


Figure 3. Scope of literature review

2.1 Examination of Contemporary Trends

2.1.1 Sustainable Construction

Sustainability is a paramount objective in construction, encompassing building creation, renovation, operation, and management. To achieve this goal, effective information exchange and robust data security are imperative. Throughout a building's life cycle, diverse and intricate data sources are employed by multiple stakeholders. Consequently, comprehending,

integrating, managing, and facilitating the sharing of this information poses a considerable challenge.

The article "Information Modelling for Sustainable Buildings" introduces the Sustainable Building Profile (SBP), an innovative conceptual model specifically crafted for integrating data related to energy efficiency and renewable energy sources (RES) within buildings (Figure 4). This SBP can be taken as a base for a Self-Sovereign Digital Wallet.

The SBP offers a framework for analyzing a building's evolution over time. Various stakeholders can leverage this model to explore a range of engineering, operational, and maintenance issues pertaining to energy efficiency in buildings (König *et al.*, 2011).

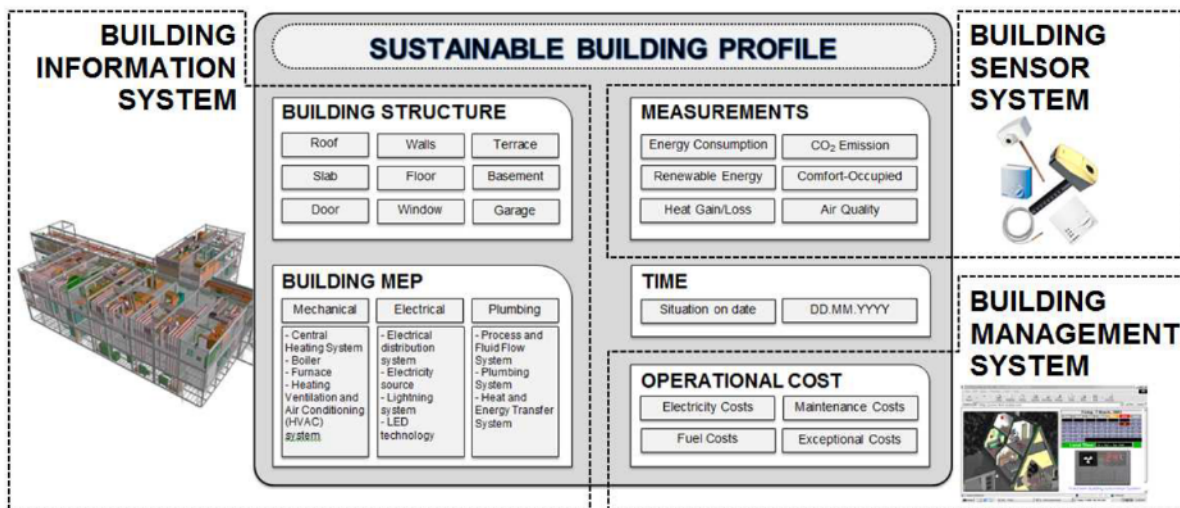


Figure 4: Sustainable building profile and related information sources - Source: (König *et al.*, 2011)

Key stakeholders encompass a wide range of participants, including producers of various renewable energy sources (RES), engineering companies providing building materials, techniques, products, and services, architects contributing to sustainable building design, manufacturers of energy-efficient machines for building use, and governmental organizations responsible for implementing regulations. To facilitate the exchange of information among these diverse stakeholders, exploring the development of a knowledge base is essential.

An SBP can effectively store a snapshot of building information at a specific point in time. Nevertheless, over the lifespan of a building, the management of multiple SBP instances, each representing the building's status at different times, becomes necessary.

2.1.2 Construction 4.0

Despite ongoing efforts to align with sustainability requirements, the construction industry is often perceived as traditional, resistant to technological advancements, and plagued by inefficiencies. However, recent technological breakthroughs have ushered in a new era in construction, referred to as "Construction 4.0." This represents a significant departure from traditional practices and emphasizes rapid growth and improved profitability, all driven by cutting-edge technology and innovation (Chen *et al.*, 2022).

The Construction 4.0 paradigm is delineated as an extension of the influential Industry 4.0 framework, which has gained prominence within the tumultuous currents of the Fourth Industrial Revolution. This framework has ignited a wave of transformation that permeates various sectors, extending its reach into the intricate tapestry of the built environment (Sawhney *et al.*, 2020).

The key components of Industry 4.0 are Internet of Things (IoT), Cyber-physical System (CPS), Cyber-Physical Production System (CPPS), and Internet of Data and Services (IoS) (Figure 5). At the core of this framework lies the IoT layer, seamlessly linking physical entities and objects, adeptly harvesting data from these interconnected elements, and facilitating fluent communication and collaboration among them. CPS layer encompasses a range of technologies that intertwine the virtual and physical realms, forging a tightly interconnected production ecosystem where intelligent entities communicate and engage harmoniously. This dynamic synergy gives rise to the CPPS layer, establishing a digitally advanced, intelligent, streamlined, service-centric, and interoperable production landscape. Simultaneously, the Internet of Services (IoS) engenders a service-oriented ecosystem, infusing customer-centricity into the very fabric of the system, empowering end-users (Hofmann and Rüsçh, 2017).

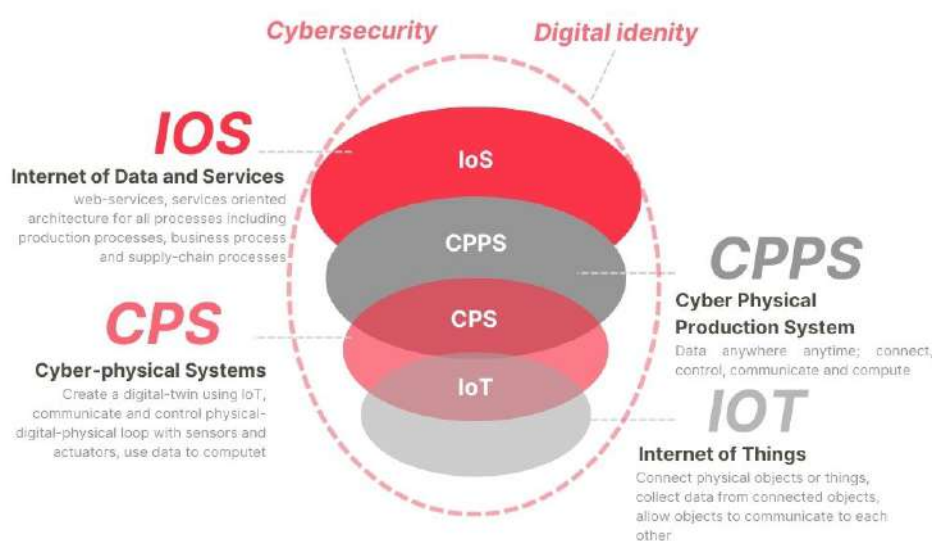


Figure 5. The key components of Industry 4.0

In construction, smart applications are essential for addressing complex challenges like safety, site management, resource optimization, waste reduction, and progress monitoring (Kochovski and Stankovski, 2021). These applications leverage four key technologies: the Internet of Things (IoT), Artificial Intelligence (AI), Cloud Computing, and Blockchain (Kochovski and Stankovski, 2020). Trust is critical in scenarios where resources from various entities, like Edge, Fog, and Cloud computing, are involved. For instance, DECENTER's Fog Computing Platform supports Big Data processing, enabling AI algorithms across this computing continuum (Kochovski *et al.*, 2019).

The increasing adoption of advanced IoT technologies, especially at the far edge of the network, has been notable in recent years (CARBONE *et al.*, 2018; Gill *et al.*, 2019). This convergence of technologies is poised to usher in a new era of advanced and intelligent applications for the construction industry, offering tremendous potential for innovation and efficiency in the near future (Kochovski and Stankovski, 2018). Ensuring secure access control for messages is a critical and ongoing challenge in the realm of smart IoT applications. In the article titled "A Capillary Computing Architecture for Dynamic Internet of Things: Orchestration of Microservices from Edge Devices to Fog and Cloud Providers," the authors highlight a potential avenue for future research. This area of investigation could focus on technologies that enhance the security of sensitive data (Tahezadeh, Stankovski and Grobelnik, 2018).

Amidst this intricate integration, cybersecurity, efficient data management and digital identity become crucial sentinels for data ownership and control. This protective synergy aligns not only with the evolving Industry 4.0 landscape but also resonates within the transformative ethos of Web3.

2.1.3 BIM

Currently, BIM has evolved into a foundational digital framework within the Architecture, Engineering, and Construction (AEC) industry (Pan and Zhang, 2023).

BIM is characterized as a collection of interconnected policies, processes, and technologies that establish a systematic method for overseeing crucial information related to building design and project data in digital form throughout a building's life cycle (Wong and Zhou, 2015). The exceptional performance demonstrated by BIM-driven project delivery in digital management has led to its widespread embrace, propelling the AEC sector towards increased levels of automation, intelligence, security, and reliability in the digital age (Jung and Lee, 2019).

Bew and Richards introduced the UK BIM maturity model, outlining distinct stages of progression (Bew, M., & Richards, 2008). This model was complemented by Erika A. Pärn and David Edwards. On this matrix the red line shows increasing risk of cyber-security attacks (Pärn, Edwards and Sing, 2017).

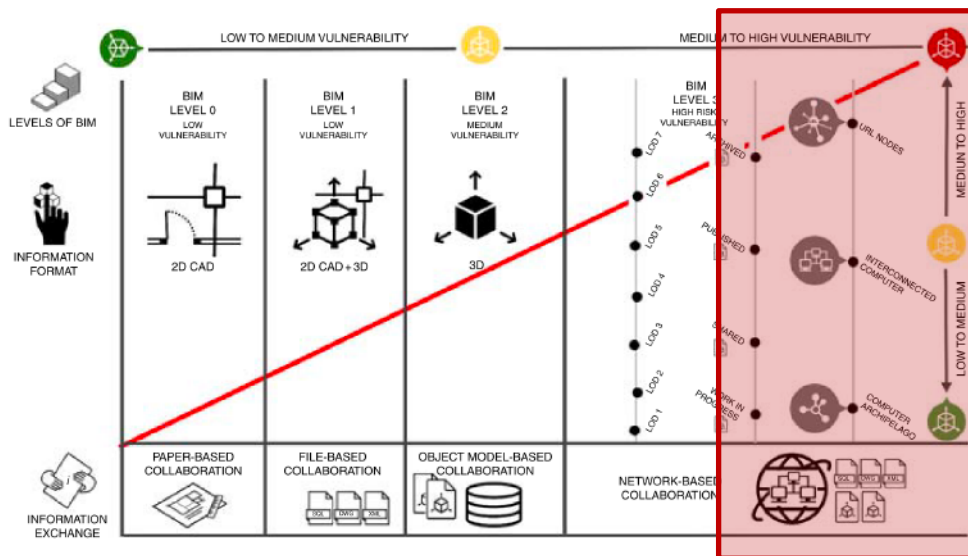


Figure 6 Cyber vulnerabilities- Source: (Pärn, Edwards and Sing, 2017)

Information regarding the structural and architectural aspects of buildings is typically stored using Industry Foundation Classes (IFC), an XML-based format widely employed by various software toolsets (König *et al.*, 2011). IFC serves as a standardized descriptive language, providing the capability to comprehensively define a building model in various formats, including RDF, SPF, XML, and JSON (Pauwels *et al.*, 2023). This allows multiple applications to access and interpret this data effectively (Krijnen and Beetz, 2018; Tang and Shelden, 2020).

Semantic Web technologies and standards, guided by W3C principles, simplify the sharing of extensive web data. Linked Data has gained significant traction as a research field within the AEC domain over the past decade. It encompasses a set of design principles aimed at facilitating the sharing of machine-readable interconnected data on the web (Bonduel *et al.*, 2018a). By representing building data, such as BIM, in the linked data format, it can be seamlessly integrated with data from other relevant sources. This integration empowers organizations to extract added value from their existing data repositories, transcending traditional boundaries and domains (Oraskari and Törmä, 2015a, 2015b; Zhu, Wu and Lei, 2023).

Pauwels *et al.* outlined multiple data transfer methods, which encompass IFC-RDF file transfer, IFC-LBD file transfer, and IFC-JSON file transfer.

- **IFC-RDF file transfer**

By introducing the ifcOWL ontology as an equivalent counterpart to the IFC schema in the OWL, the possibility to represent such models in RDF, a versatile information modeling approach, is made available. These models can then be queried using SPARQL.

- **IFC-LBD file transfer**

A similar methodology is employed to convert IFC data into modular Linked Building Data (LBD) graphs, initially focusing on the BOT, PROPS, and PRODUCT ontologies (Figure 7). This process involves the extraction of relevant information from IFC building models and its transformation into streamlined Abox RDF graphs, perfectly suited for use in Linked Data applications. (Bonduel *et al.*, 2018b).

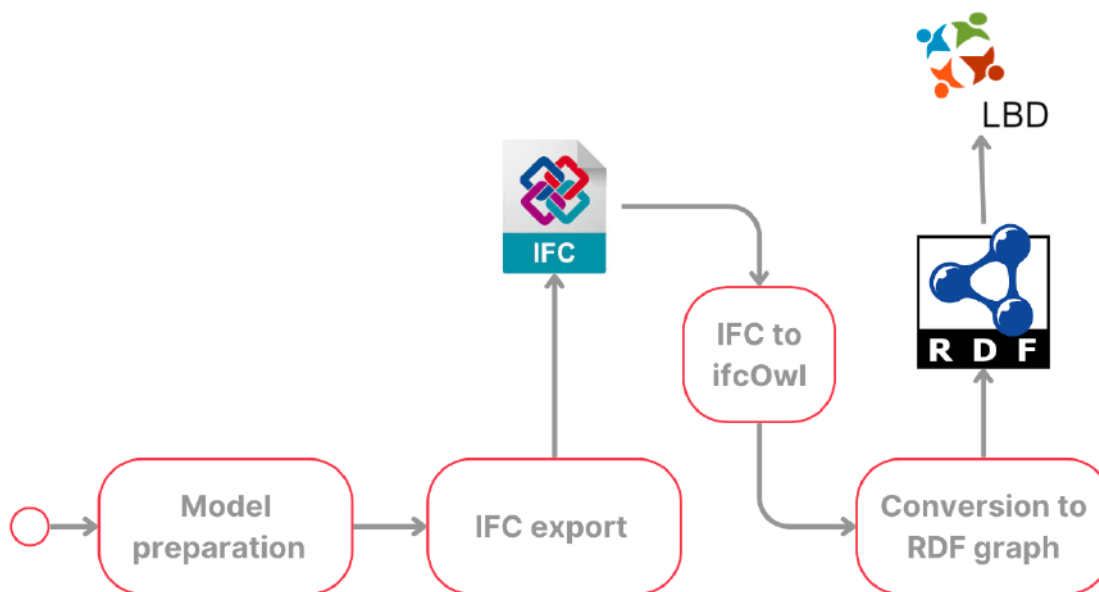


Figure 7: IFC to LBD conversion process

- **IFC-JSON file transfer**

The JSON format of IFC can also be employed. JSON is considered a versatile data format that is widely used in modern web services and platforms. It boasts strong compatibility with various software libraries and contemporary development practices.

The Workshop on "Supporting Decision-Making in the Building Life cycle using Linked Data" showcased several contexts where linked data and semantic web technologies could offer substantial benefits to AEC experts. These approaches typically initiate from the IFC schema, and an IFC-to-RDF conversion service can be deployed to transform IFC data into RDF representations. Assuming similar RDF conversion services can be established for other schemas commonly used in the AEC realm, one can envision diverse information models available as RDF graphs within a single building project. Expanding the linked data ecosystem for AEC projects to encompass connections with sensor data, operation and maintenance manuals, financial records, and weather data has the potential to enhance building performance during the maintenance phase of the building life cycle (Figure 8) (Pauwels, 2012).

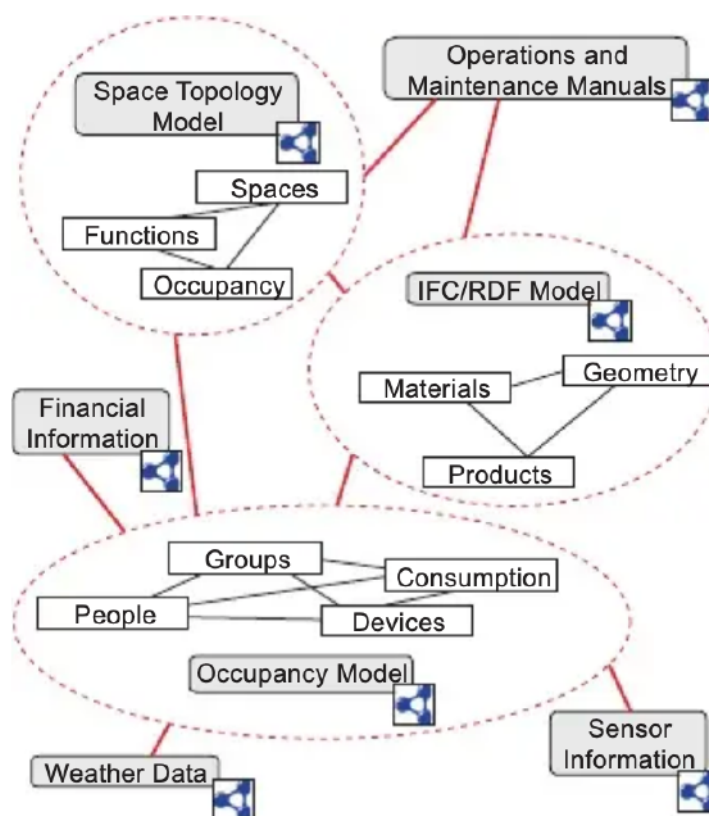


Figure 8: The linked data cloud for the AEC project – Source: (Pauwels, 2012)

2.1.4 A Brief Overview of Web3

The worldwide advancements, particularly in Information and Communication Technologies (ICTs), have significantly impacted modern society. These developments in ICTs have transformed people's perspectives in various ways. ICTs serve as effective tools for providing communication and information services to individuals. One of the most significant changes brought about by ICTs is the widespread adoption of the World Wide Web, revolutionizing how people access information and communicate with one another (Hiremath and Kenchakkanavar, 2016).

Recent progress in Information Technology has not only enhanced global access, storage, and processing of information but has also led to significant changes in concepts, advanced services, and management practices.

Web3's central idea revolves around decentralizing data and establishing a token-based economy. (Buldas *et al.*, 2022) This upcoming web phase is poised to revolutionize the real estate and construction industries, streamlining property operations for businesses.

The BUILDCHAIN initiative is set to establish a scalable, BIM-based decentralized knowledge platform that digitally identifies, registers, updates, and analyzes extensive datasets related to the entire life cycle of buildings. This platform will be developed using the Origin Trail Decentralized Knowledge Graph. Within the BUILDCHAIN project, a Digital Building Logbook solution will be designed and implemented to integrate building data and knowledge. This logbook will also introduce new applications and features aimed at enhancing integrated information, efficiency, sustainability, and transparency, ultimately improving the building stock. The Digital Building Logbook proposes a unified European approach to aggregate pertinent building data, ensuring authorized parties have access to accurate building information. Target users include market participants such as property owners, tenants, investors, financial institutions, and public administrations (Serrano, 2023).

This aligns synergistically with Web3's vision of data decentralization. The potential for SSI to harmonize with the impending transformation of real estate and construction sectors underscores a realm where secure and verifiable identity management intertwines with decentralized data structures.

2.2 Overview of Digital Identity

In the modern era, digital identity holds considerable importance for individuals, organizations, governments, and entities, forming an essential foundation for conducting transactions (Simmonds, 2015). Traditionally, contractual agreements, trade, and exchanges primarily occurred in face-to-face interactions. However, the current landscape witnesses a significant shift towards digital transactions. This shift necessitates the presence of a digital identification or authentication mechanism, referred to as digital identity (Clauß and Köhntopp, 2001; Goode, 2019). This digital identity serves the purpose of accurately identifying individuals, devices, or objects within the virtual realm, facilitating seamless interactions among various stakeholders (Ante, Fischer and Strehle, 2022).

Lennart Ante identified and classified seven separate research streams along with their interconnections using co-citation analysis, naming these seven research streams as depicted in Figure 9 (Ante, Fischer and Strehle, 2022).

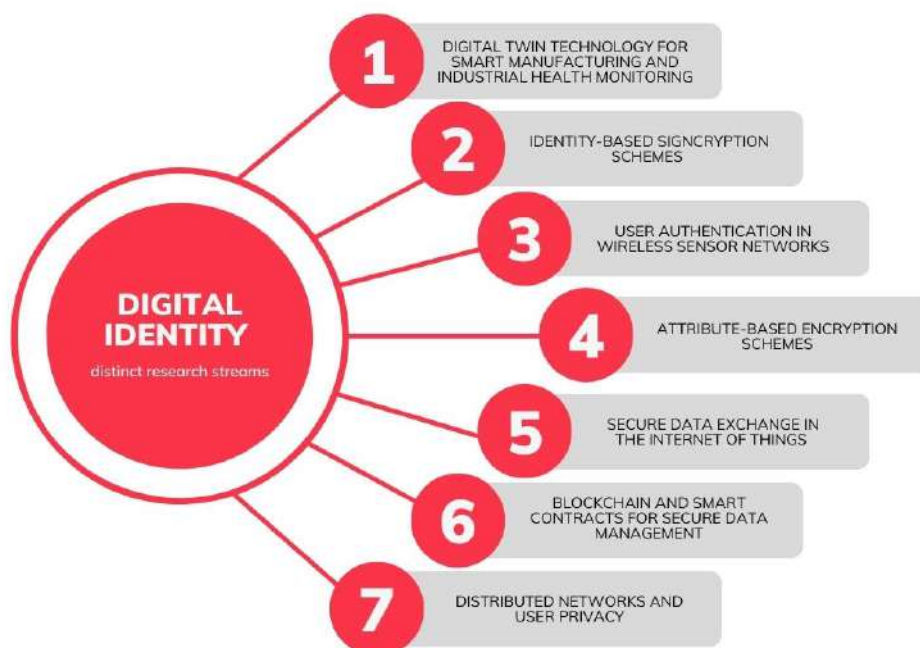


Figure 9. Seven separate research streams- Source: (Ante, Fischer and Strehle, 2022)

As previously noted, as the adoption of Construction 4.0, Web3, and BIM Level 3 gains momentum in the construction industry, the establishment of a decentralized identity system is crucial, as it allows users to possess SSI, granting them absolute control over their data. This empowers individuals with greater autonomy and security over their personal information, fostering a more user-centric and privacy-focused online experience (Wang, Zhang and Liew, 2023).

The conventional digital identity framework is gradually proving insufficient for the evolving needs of the modern construction industry. The shortcomings of the traditional centralized identity management system are increasingly apparent. For instance, individuals lack genuine control over their digital identities, rendering them susceptible to the potential exposure and theft of identity-related information. In contrast, the attributes of Web3 technology, encompassing decentralization, tamper-proof mechanisms, traceability, and more, offer promising solutions to the predicaments posed by centralized digital identity (Bai *et al.*, 2022).

2.2.1 The Evolution of Digital Identity

In our daily lives, we frequently rely on documents like passports and driver's licenses to verify our identities in the physical world. However, as more processes shift into the digital domain,

there's a growing need to establish and validate our identities in the online space (Preukschat, Alex, 2021).

In essence, a digital identity pertains to the intrinsic nature of an entity, object, or subject. An entity, whether it exists in the physical or digital realm, possesses a singular digital identity, which may encompass a series of descriptors characterizing it. Notably, an individual's identity can be a subset of an organizational or device identity, for example, a wallet within a vehicle. Practical implementation entails utilizing partial identity subsets, as diverse services require distinct identifiers.

Regarding methods of identification, these fall into three categories:

1. Single identifiers, which encompass attributes like nationality or a device's manufacturer, constituting information that lacks exclusivity.
2. Unique identifiers, exemplified by product serial numbers.
3. Secure identifiers, such as passports or smart meters.

These types of information can be employed as identifiers in online contexts, permitting the verification of a subject's authenticity across a computer network through one or more identifiers (Ante, Fischer and Strehle, 2022).

Figure 10 illustrates a compilation of attributes that are digitally recorded and stored. These attributes, including details like name, date of birth, and gender, are coupled with credentials associated with a distinct identifier. This identifier serves the purpose of uniquely identifying an individual, enabling seamless transactions within the digital realm.

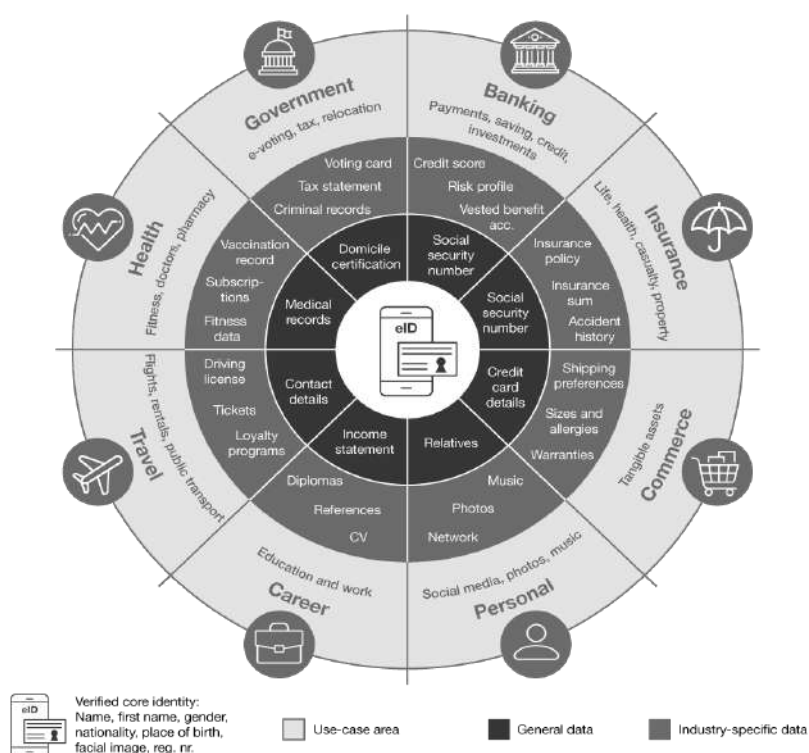


Figure 10: A compilation of attributes that are digitally recorded and stored for different use-cases - Source: PwC

The rise of new technologies necessitates a fresh perspective on establishing secure connections for accessing and safeguarding private information, prompting a shift from traditional paper-based identities to their digital equivalents. The evolution of digital identity has traversed various phases, encompassing the centralized identity model, federated identity model, and decentralized identity model. Figure 11 provides a visual representation of the progression of digital identity over the years (Bai *et al.*, 2022).

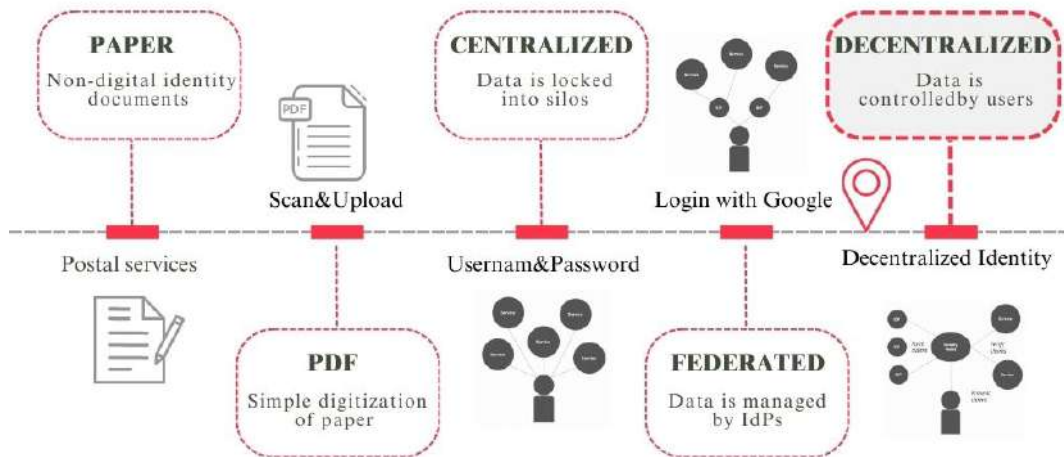


Figure 11: Digital identity models

Y. Jing, J. Li, Y. Wang and H. Li, described digital identity models (Y. Jing, J. Li, 2021):

1. Centralized identity model

This centralized strategy reduces the need for repetitive data input and delivers a user-friendly encounter by reutilizing stored details—an approach that remains common in contemporary internet applications. The establishment of the centralized identity model involves creating an account with a website, service, or application (Figure 12).

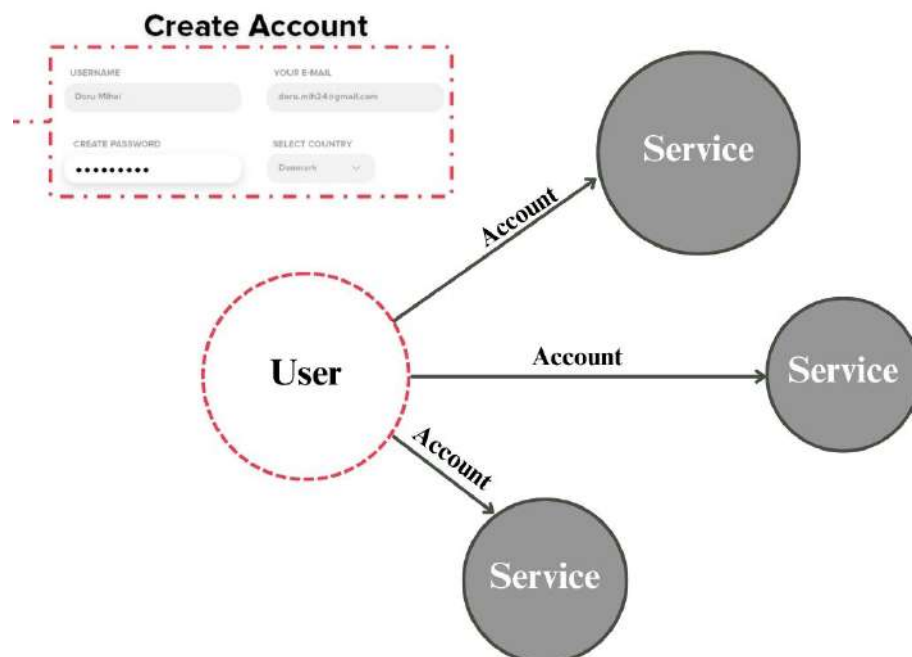


Figure 12: Centralized identity model

2. Federated identity model

This approach diverges from the centralized model by incorporating Identity Providers (IDPs), facilitating simplified creation, management, and maintenance of online identities. IDPs also offer authentication services for third-party network applications, enabling users to achieve one-click login or trusted network providers (Y. Jing, J. Li, 2021) (Figure 13).

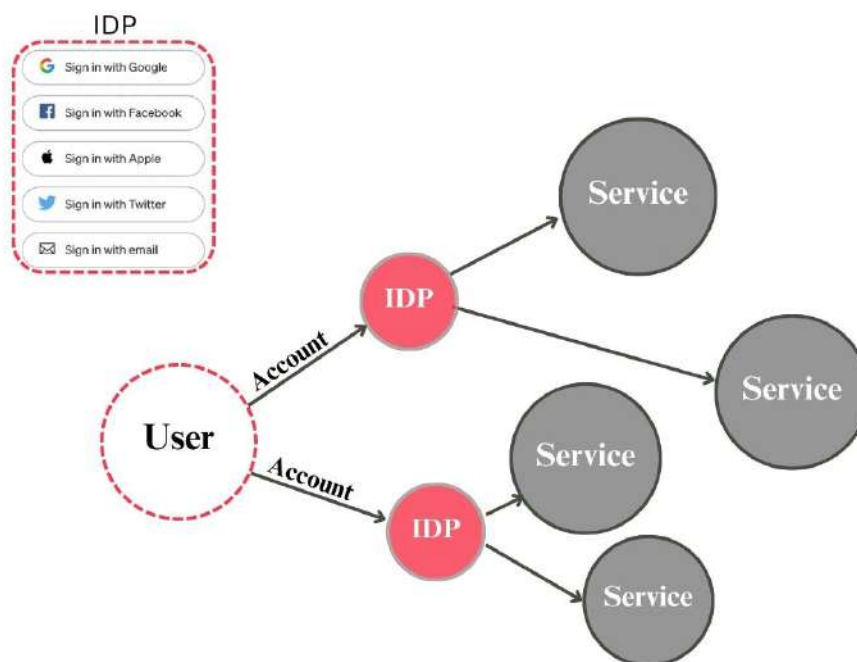


Figure 13. Centralized identity model

3. Decentralized identity model

In 2015, a novel model surfaced, drawing inspiration from blockchain technology. This model abandoned the reliance on centralized or federated identity providers and embraced a fundamentally decentralized approach. Its evolution was swift, absorbing advancements in cryptography, distributed databases, and decentralized networks. This transition gave birth to groundbreaking decentralized identity standards, including Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs) (Reed, Allen and Vogelsteller, no date).

The most significant departure of this model lies in its departure from an account-based structure. Instead, it mirrors real-world identity dynamics, fostering direct peer-to-peer relationships between individuals, eliminating the notion of either party "providing," "controlling," or "owning" the relationship. (Preukschat, Alex, 2021) This peer-to-peer interaction occurs within a decentralized platform, bypassing the need for centralized

accounts. Users upload public keys for identity verification onto the blockchain, ensuring secure verification through encryption and private peer-to-peer connections (Y. Jing, J. Li, 2021) (Figure 14).

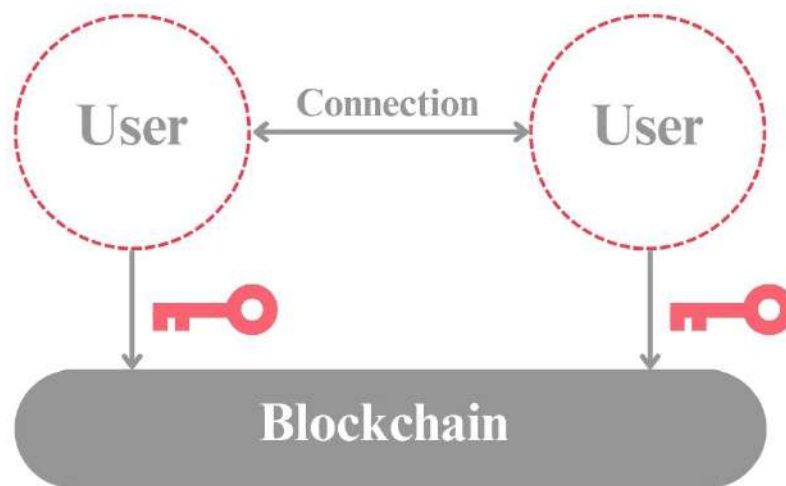


Figure 14. Decentralized identity model

The most fitting analogy for the decentralized identity model is essentially how we authenticate ourselves daily in the physical world – by presenting credentials from trusted sources in our wallet. In the decentralized digital identity context, this process transpires through digital wallets, credentials, and connections.

The term used to describe the decentralized identity model is "self-sovereign identity" (SSI), which made its appearance on the internet scene in 2016. SSI encompasses principles guiding the functioning of identity and personal data control across digital networks. It's also a collection of technologies built upon key concepts in identity management, distributed computing, blockchain or distributed ledger technology (DLT), and cryptography (Preukschat, Alex, 2021).

2.2.2 Use Cases

SSI offers numerous advantages for organizations, allowing them to enhance their offerings, streamline operations, and mitigate various business risks:

1. Improved Conversion and Stakeholder Satisfaction: Organizations can provide their stakeholders with smoother access to services or products, leading to higher conversion rates, reduced help desk requests, and overall increased stakeholder satisfaction.

2. Enhanced Data Quality: SSI empowers organizations to receive dependable data about their stakeholders, which is verified and signed by trusted third parties, ensuring data accuracy.
3. Prevention of Fraud: Organizations can proactively prevent various forms of malicious activities, ranging from spam to identity theft and document forgery, safeguarding their operations.
4. Heightened Security: By eliminating risk factors like passwords and adopting decentralized data storage, organizations can mitigate the risk of data breaches and enhance overall security.
5. Compliance: SSI inherently supports compliance with privacy and data protection regulations by prioritizing user-centric data control and consent management, helping organizations meet regulatory requirements effectively.

Dimitrios A. Maniatis introduces a cybersecurity framework integrating SSI into marine wind turbines applicable in Greek waters. The proposed system incorporates numerous sensors for data collection, interconnected with an intelligent system that makes decisions based on contextual situations (Maniatis, 2022).

Cocco Luisanna, Tonelli Roberto, and Marchesi Michele suggested a system proposal that utilizes SSI principles to digitize construction processes. This proposal integrates Blockchain, BIM, IoT devices, and SSI concepts. It accurately identifies stakeholders, efficiently manages data, and employs off-chain storage for most information and on-chain storage for notarization and certification. Multi-signature approval mechanisms enhance security, and the system verifies certified data eligibility, benefiting facility management. (Cocco, Tonelli and Marchesi, 2022).

Luca Giorgino proposed the development of an edge device designed to securely assist constrained devices in establishing and managing their own identity, following the principles of SSI. The software for this edge device was created using Keystone, an open-source framework designed for constructing Trusted Execution Environments. This edge device facilitates the establishment of a trusted communication channel between IoT devices and the edge device itself, which is responsible for managing offloaded operations (Torino, 2022).

The walt.id website showcases numerous use cases that highlight the significance of digital identity in various domains. Digital identity is crucial for governments and businesses across all sectors and industries, making its applications virtually limitless (Figure 15).

eCommerce	Frictionless check-out.	Vouchers, discounts (e.g. for students)	Proof of age (e.g. tobacco, alcohol).
Travel & Mobility	Application / verification of visas.	Hotel booking and check-in/out.	Vaccination proofs, transportation tickets.
Health Care	Proof of insurance.	Digital prescriptions and medical reports.	Proof of vaccination.
Supply Chain	Verification of product authenticity.	Verification of product provenance, lifecycle.	Verification of vendors, other actors.
Marketplaces	Frictionless user onboarding and authentication.	Fraud prevention via user verification and identification.	Automated data provision (right to access).

Figure 15: The walt.id website use cases

It was noted that there was a lack of extensive research on the management of data using SSI in the context of construction projects. Recognizing this research gap as an opportunity, a case study was developed to test the proposed framework.

3 TECHNOLOGY BACKGROUND: SELF-SOVEREIGN DIGITAL IDENTITY

As previously mentioned, at the core of this model lies a peer-to-peer relationship. Unlike traditional identity models that commonly involve transmitting a username and password (or its hash) to a remote application for user authentication, decentralized identity models operate differently.

In decentralized identity models, when establishing a new peer relationship, the identity owner and the remote application securely exchange unique DIDs. These DIDs are specific to the relationship and are known as pairwise DIDs. Significantly, these pairwise DIDs are kept exclusively between the parties engaged in the interaction and are never publicly shared on a ledger. They are used exclusively during encrypted operations conducted between the parties.

By privately negotiating and utilizing pairwise DIDs, external entities like public key servers or messaging hosts are unable to access the keys or plaintext messages. This method ensures robust end-to-end encryption, as encryption remains confined to the two parties participating in the peer relationship.

There are three main pillars of SSI standardization which are DID and VCs and Decentralized Ledger (Figure 16).

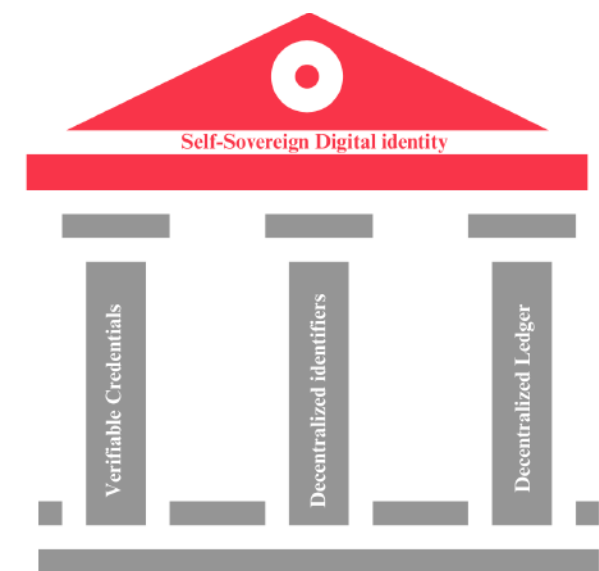


Figure 16: The three pillars of SSI

The SSI data model proposed by the European Blockchain Services Infrastructure (EBSI) aims to provide a framework for Self-Sovereign Identity (SSI) within the European Union, as depicted in Figure 17.

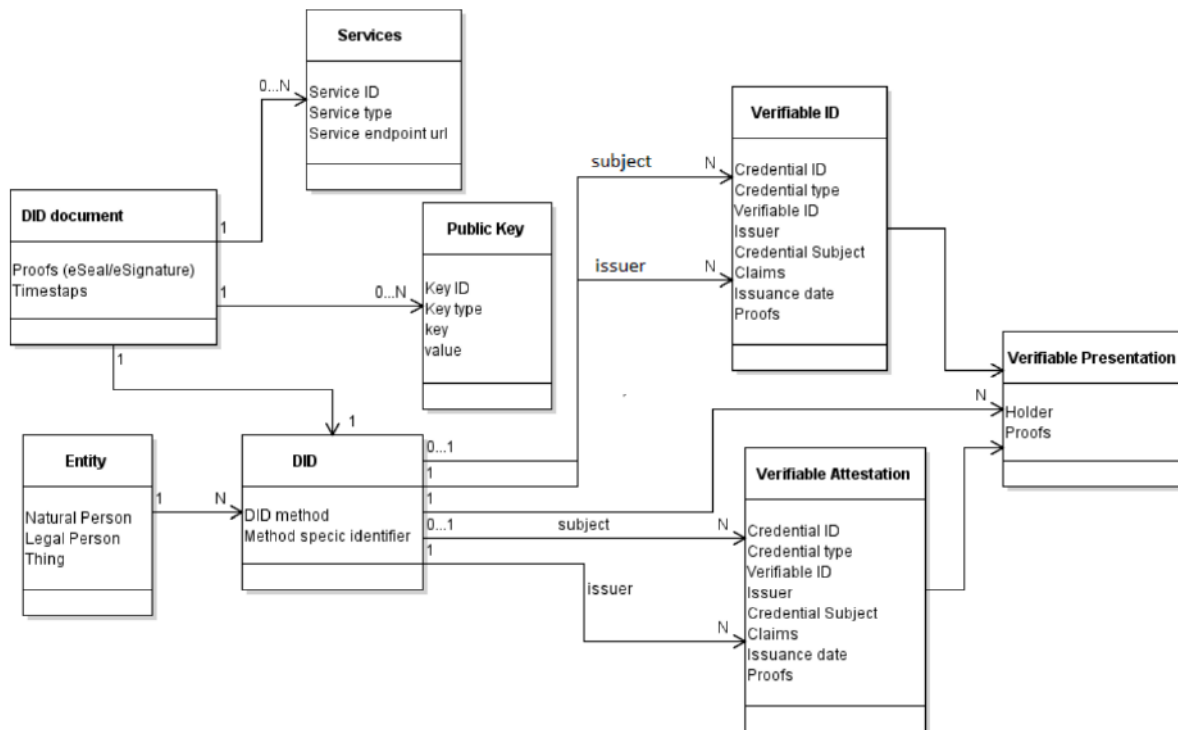


Figure 17: SSI data model - Source: EBSI

3.1 SSI Architecture

In 2019, SSI architects from diverse backgrounds collaborated within the Hyperledger Aries project to create the four-layer paradigm, as depicted in Figure 18. This paradigm is the framework we reference throughout this chapter. While the lower layers serve as essential infrastructure, the upper layers encompass user-visible concepts.

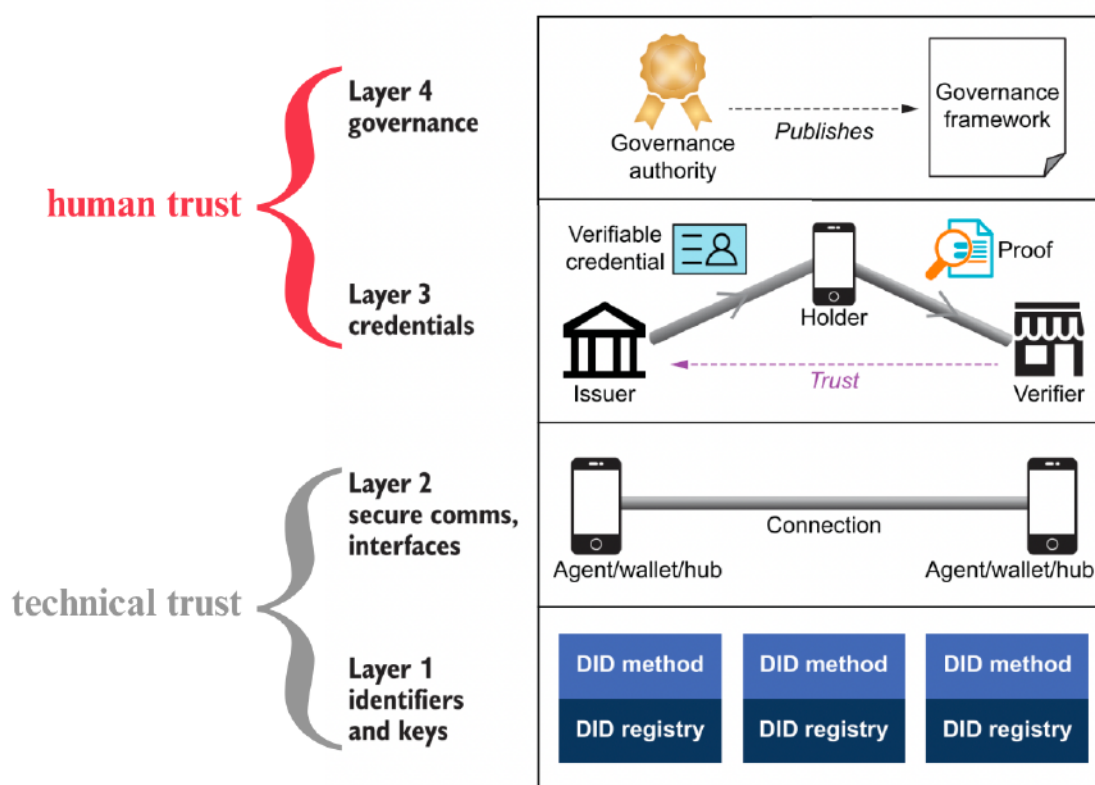


Figure 18: The SSI stack as a four-layer model

Layer 1, situated at the stack's base, handles the definition and management of identifiers and public keys. The SSI community generally advocates the use of a verifiable data registry, often referred to as a DID registry or DID network. These serve as decentralized sources of truth for decentralized identifiers. Each DID registry employs a DID method, outlining a protocol specific to that type of DID registry.

Layer 2 focuses on establishing trustworthy communication among the involved peers. Here, digital agents, wallets, and encrypted data stores come into play, forming secure DID-to-DID connections. After establishing a peer DID connection via the exchange of DIDs and DID documents, the resulting channel becomes a versatile means for various agent functions. This channel can be utilized for tasks such as issuing credentials, presenting, or proving credentials, data exchange, secure human messaging, and more.

Layer 3, housing the verifiable credential trust triangle, operates with a straightforward credential-sharing model used by entities like uPort, Digital Bazaar, Microsoft, and others. During credential presentation, the holder discloses the entire credential, including this DID.

Ownership of the credential is proven by demonstrating control over the cryptographic keys linked to this DID. Credential revocation in this context is managed via revocation lists.

Layer 4 acts as the bridge connecting the technical aspects of the SSI stack with the real-world business, legal, and social requirements of SSI solutions, shifting the focus from technology to human and policy considerations.

3.2 Verifiable Credentials

Credentials encompass any collection of information that an authority asserts as true about the subject of the credential. For example, a student identity card issued by a university serves as evidence of an individual's enrollment in the university, or a manufacturer has the capability to issue a credential related to an IoT sensor device (Reed, Allen and Vogelsteller, no date).

The origins of what are currently known as verifiable credentials trace back to a development stemming from the Web Payments Interest Group within the World Wide Web Consortium (W3C). The W3C, responsible for establishing standards for web interoperability, including the HTML web programming language, played a crucial role in shaping this concept.

A verifiable credential can encompass the entirety of information that a physical credential holds. The incorporation of technologies like digital signatures enhances the tamper-evident nature and trustworthiness of verifiable credentials, surpassing the reliability of their physical counterparts (*Verifiable Credentials Data Model v1.1 W3C Recommendation 03 March 2022*, no date).

Verifiable credentials in the context of construction services enable individuals to communicate trustworthy and authenticated information to parties requesting it, who can then confirm the accuracy of the shared data. The versatility of verifiable credentials extends to supporting critical qualifications specific to the construction industry, such as certifications, licenses, and project credentials. Additionally, the integration of verifiable credentials has the potential to simplify routine authentication processes and data sharing within construction workflows.

Figure 19 illustrates basic components of verifiable credentials.



Figure 19: Basic components of a verifiable credential

Credentials could encompass an identifier along with metadata aimed at detailing specific attributes of the credential. These attributes might comprise information about the issuer, expiration date and time, a visual representation, a public key for verification, the mechanism for revocation, and other pertinent details. The issuer might also sign the metadata for added authentication.

3.2.1 Claims

One of the main parts of the VCs is a claim. The claim constitutes a statement concerning a subject, which is an entity that claims can be attributed to. These claims are formulated through subject-property-value relationships, where the subject is the entity in question, and the properties and values represent the aspects being asserted. The basic structure of a claim is presented on Figure 20.

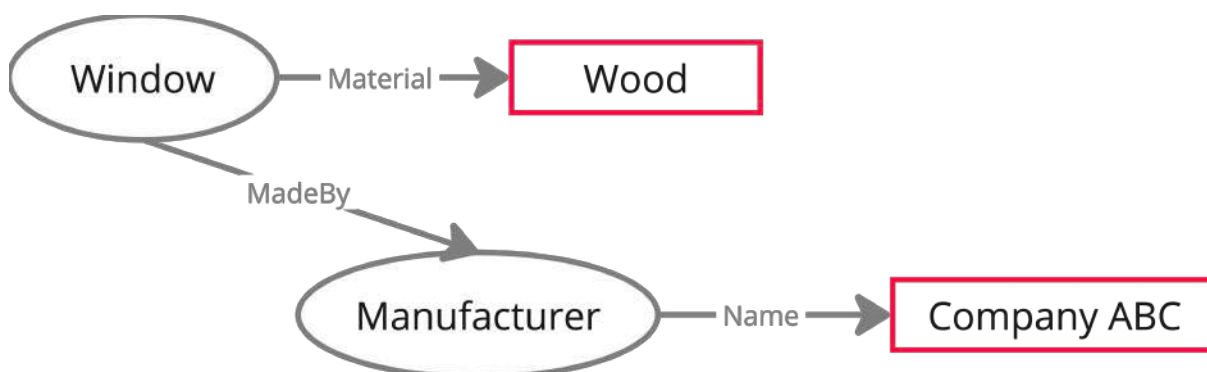


Figure 20: The basic structure of a claim with various aspects of a subject

3.1 Verifiable Presentation

A verifiable presentation (VP) consolidates information from one or more VCs and is structured to ensure the verifiability of data origin. When verifiable credentials are presented directly, they transform into verifiable presentations. Moreover, data formats built upon the cryptographic verifiability of verifiable credentials, though not inherently containing verifiable credentials, can also qualify as verifiable presentations. Basic components of a VP are:

- Presentation Metadata
- Verifiable Credential(s)
- Proofs

While the data in a presentation often pertains to the same subject, it may originate from various issuers. This aggregated information commonly portrays an aspect of an individual, organization, or entity.

3.2 Syntactic Representations

VCS, VPs and DIDs utilize JSON, a serialization format that is not only easy for humans to read but also lightweight for parsing. It can be tailored into two specific formats: JSON Linked Data (JSON-LD), a serialization format for linked data; and JSON Web Token, a commonly employed format for expressing security claims (Fedrecheski *et al.*, 2020).

Figure 21 illustrates an example of JSON-LD syntactic representations of a verifiable credential.

```

VCCCCBuildingElementsTemplate > No Selection
1 {
2   "@context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://example.com/context/building-elements-v1.jsonld"
5   ],
6   "id": "urn:uuid:7893f2d7-1a85-43c1-8b81-61b79bb674c1",
7   "type": ["VerifiableCredential", "BuildingElementsCredential"],
8   "issuer": "did:example:issuer",
9   "issuanceDate": "2023-08-26T14:30:00Z",
10  "expirationDate": "2024-08-26T14:30:00Z",
11  "credentialSubject": {
12    "id": "did:example:elementdid",
13    "claims": {
14      "ElementName": "Roof",
15      "Material": "Concrete",
16      "Dimensions": "10m x 5m x 0.2m",
17      "Sustainability": "Recyclable",
18      "Manufacturer": "Acme Building Supplies",
19      "FireRating": "Class A"
20    }
21  },
22  "proof": {
23    "type": "Ed25519Signature2018",
24    "created": "2023-08-26T14:45:00Z",
25    "proofPurpose": "assertionMethod",
26    "verificationMethod": "did:example:issuer#keys-1",
27    "jws": "eyJhbGciOiJIJFZERTQ5J9..."
28  }
29 }

```

Credential Metadata
 Claims
 Proofs

Figure 21: A syntactic representations of a verifiable credential

3.3 Roles of Self-Sovereign Identity

As was mentioned before, the structure of the SSI environment is established as a peer-to-peer model, where individual identities function as peers and interact with one another. This communication enables individuals and organizations to validate information through the assignment of claims or credentials from individuals (Nagaroor, 2008).

Shuaib, Mohammed, et al. outlined the key components of SSI as the identity verifier, identity issuer, and credential issuer. These entities' functions are depicted in Figure 22. This figure illustrates the terminology defined by the W3C Verifiable Claims Working Group for the three primary roles involved with the exchange of VCs:

1. Issuer:

The role of an issuer involves an individual, a trusted organization, or an entity that validates a user's assertions regarding their identity and issues a digitally signed credential to them. Each credential comes with a specific issuer associated with it.

2. Holder:

The holder is an individual, an organization, or an entity that possesses the verifiable credential and stores it within their digital wallet. This digital wallet is typically an application accessible only to the user, secured by a PIN or a distinct biometric identifier exclusive to them.

3. Verifier:

A verifier is a trusted entity or organization that seeks to authenticate a holder's credential. Upon receiving the credential, the verifier evaluates whether the claims within the credential meet the stipulated criteria. Verifiers request proofs from holders, encompassing claims from one or more verifiable credentials. If the holder agrees, their representative responds with a proof that the verifier can subsequently verify. A pivotal step in this process is the verification of the issuer's digital signature, usually accomplished using a DID.

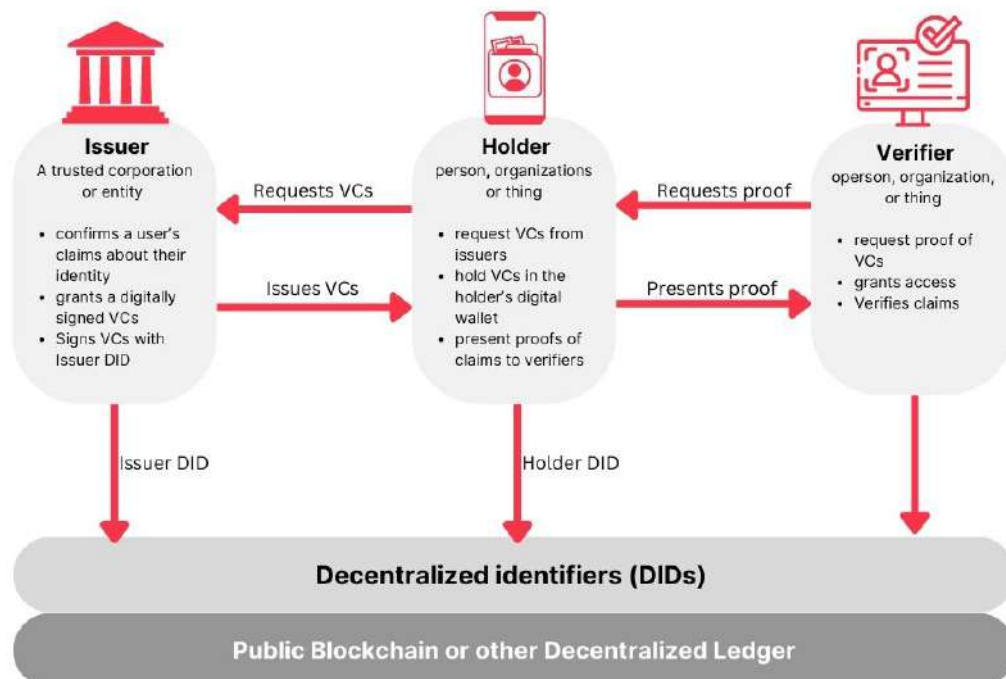


Figure 22: Roles of Self-Sovereign Identity

The trust triangle captures the interaction among issuers, holders, and verifiers, reflecting how trust relationships are established in a digital network. In numerous business interactions, both involved parties seek information from each other, meaning that within a single transaction, both parties assume the roles of holder and verifier.

3.4 Decentralized Identifiers

Both individuals and organizations frequently rely on globally unique identifiers across various applications. These identifiers function as communication addresses, including telephone numbers, email addresses, and social media usernames. They also serve as identification numbers, such as those found on passports, tax IDs, and health insurance cards.

DIDs represent a novel form of identifier that facilitates verifiable and decentralized digital identity. DIDs can be applied to identify various subjects, such as individuals, organizations, objects, data models, or abstract entities, and their control is determined by the DID controller.

As the creation and validation of DIDs are under the control of the respective entities, each entity has the flexibility to generate as many DIDs as needed to manage various aspects of their identities, personas, and interactions. These identifiers can be tailored for specific contexts, allowing entities to engage with others, institutions, or systems, asserting their identities or control over certain assets, all while retaining the ability to regulate the extent of personal or private information disclosed. Importantly, this independence from a central authority ensures that the identifier's existence is not contingent on any external entity, offering self-reliance in identity management.

In simple terms, it is like URLs we use to get access to any web page on the Internet. A resource is anything that can be identified, from a web page to a service or building element (Figure 23).



Figure 23 An example of a browser address bar displaying the URL for the web page

According to the W3C DID Core 1.0 specification, established by the W3C DID Working Group, a DID is a novel form of globally unique identifier represented as a character string that serves to identify a resource (Figure 24).



Figure 24: The format of DID

These globally unique identifiers are engineered to empower individuals and organizations to create their own identifiers through trusted systems. These new identifiers facilitate entities in demonstrating control over them by undergoing authentication processes that involve cryptographic proofs like digital signatures.

The major components of Decentralized Identifier architecture are presented in the figure below.

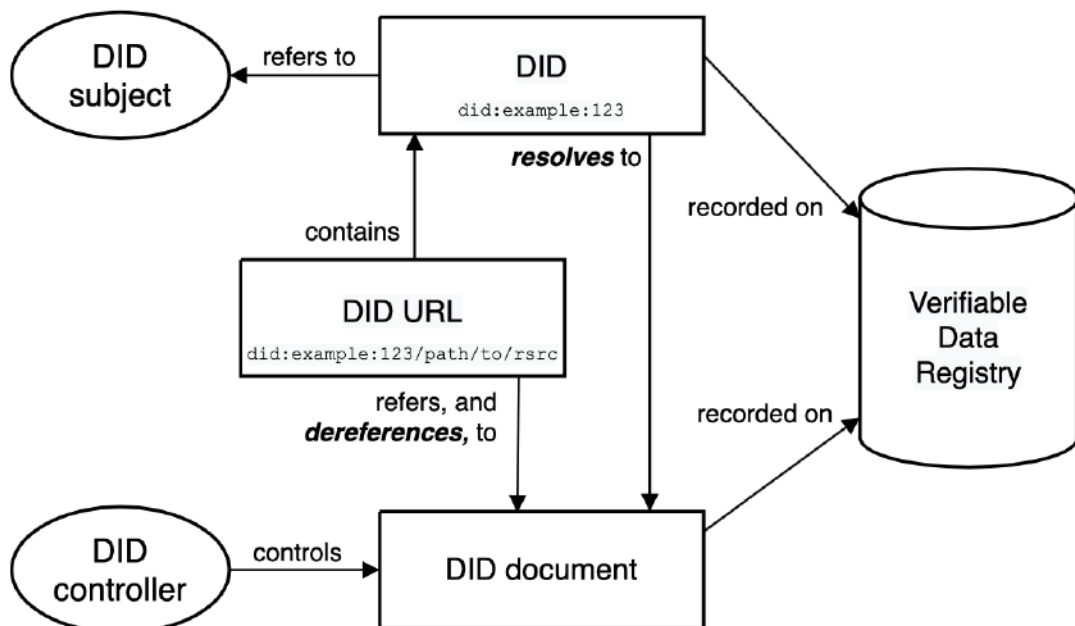


Figure 25: The major components of Decentralized Identifier architecture – Source: (Reed, Sporny and Allen, 2019)

3.4.1 DID Document

A DID document is a machine-readable file tailored for consumption by digital identity applications or services like digital wallets, agents, or secure data repositories, all of which utilize DIDs as fundamental components. Each DID corresponds to precisely one associated

DID document, housing metadata concerning the DID subject – the entity identified by the DID and expounded upon within the DID document (Figure 26). A widely advocated best practice is to include solely the essential machine-readable metadata in a DID document, just enough to facilitate reliable interactions with the DID subject.



Figure 26: Relationships between DID, DID subject and DID document – Source: (Reed, Allen and Vogelsteller, no date)

For instance, a DID assigned to a service (the DID subject) is paired with a DID document typically containing cryptographic keys, authentication methods, and additional metadata outlining the protocols for secure interactions.

The entity in charge of the DID and the corresponding DID document is referred to as the DID controller. In numerous instances, the DID controller is identical to the DID subject, although it's possible for them to be distinct entities.

For instance, consider a scenario where a company manages a DID identifying their services – here, the service serves as the DID subject, but the DID controller remains the company.

3.4.2 DID Methods

The SSI community currently encompasses a variety of DID types, each sharing core functionality but differing in their implementation. These distinctions are known as DID methods, with the DID method name situated between the first and second colons in the DID identifier format.

Here are example DIDs generated using three different DID methods:

- Sovrin (sov): did:sov:WRfXPg8dantKVubE3HX8pw
- Bitcoin (bcr): did:bcr:xyv2-xznm-qm6
- Ethereum (ethr): did:ethr:0x123456789abcdef

The actions that are envisioned to be supported by DIDs in the context of earlier work by the Credentials Community Group can be categorized into five groups: Create, Use, Read, Update, and Delete. These actions are essential for the proper functioning and management of DIDs within the SSI ecosystem.

3.5 Digital Wallets and Agent

In the physical world, we often keep our credentials in a physical wallet. This wallet serves several essential functions: it consolidates our important items in one place, safeguards them by being close to us physically, and offers easy accessibility when necessary. The role of a digital wallet mirrors this: it serves as a repository for digital credentials, keys or keycards, financial records, and more (Tobin and Reed, 2017).

Its key functions are to:

1. **Consolidate Information:** Like a physical wallet, a digital wallet gathers and organizes various digital items, such as credentials, keys, bills, or receipts, into one centralized location.
2. **Security:** It provides security measures to protect these digital assets from theft or unauthorized access, akin to a physical wallet safeguarding its contents from prying eyes.
3. **Accessibility:** A digital wallet ensures that your digital possessions are readily available and easily portable across all your devices, just as a physical wallet allows you to carry your important items wherever you go.

Abylay Satybaldy assessed the usability of SSI digital wallets, including Trinsic, Connect.me, Esatus, and Jolocom Smartwallet, to identify potential adoption obstacles. Using a cognitive walkthrough method, the study found usability issues in fundamental tasks, emphasizing the need for improvements to enhance user experience and adoption (Satybaldy, 2023).

Digital wallets in the SSI infrastructure rely on software known as a digital agent. The agent is a digital guardian that safeguards and ensures exclusive access to your digital wallet, protecting your verifiable credentials and cryptographic keys.

In the SSI infrastructure, agents have a dual role. Apart from assisting identity owners in wallet management, they communicate with each other over the internet, establishing connections and sharing credentials as per their owners' instructions. This communication takes place through a decentralized and secure messaging protocol specifically designed to ensure private interactions between digital agents.

4 CASE STUDY: SELF-SOVEREIGN DIGITAL WALLET FOR AEC INDUSTRY

This case study is part of the BUILDCHAIN project, which strives to establish a decentralized data ecosystem management system utilizing blockchain technology. The incorporation of SSI into BUILDCHAIN empowers authorized users to maintain control over their digital identities while securely accessing precise building information. This integration not only advances BUILDCHAIN's goals of enhancing the building stock and sustainability but also ensures data privacy and the creation of secure data exchange channels, ultimately reshaping the landscape of digital building data management and promoting transparency and trust within the industry.

In this system proposal, we employ DIDs to uniquely identify Construction stakeholders (Figure 27). These DIDs enable secure sharing of project-related VCs among stakeholders through protected digital channels. This approach aligns seamlessly with the principles of the Integrated Project Delivery (IPD) process.

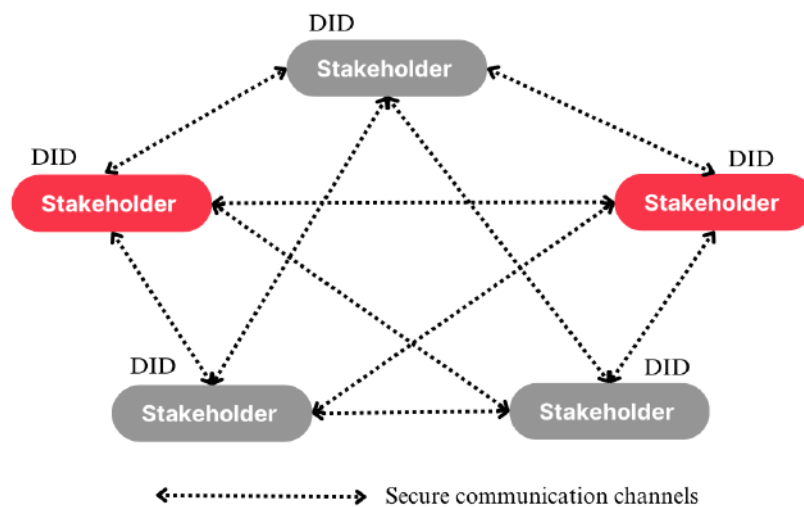


Figure 27: Data sharing through protected digital channels

It was decided to focus on two roles for implementing Self-Sovereign Digital Wallet in the AEC industry (Figure 28):

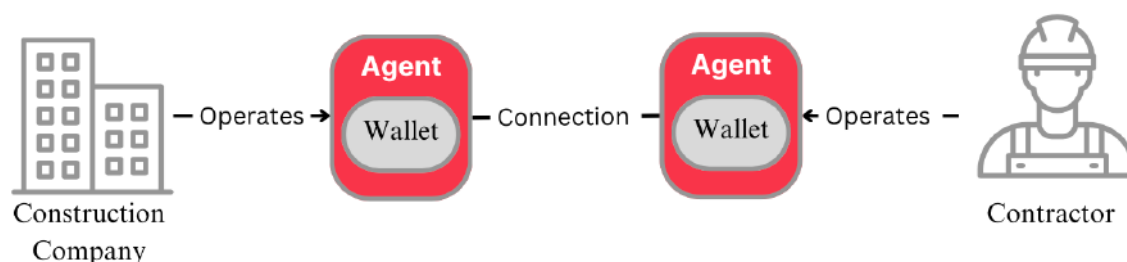


Figure 28: SSI connection

Contractors: SSI can empower contractors within the AEC field to effectively manage their VCs. These credentials may include licenses, work permissions, and various other qualifications relevant to their professional roles. Contractors can utilize these credentials not only for personal record-keeping but also to apply for construction services securely. Additionally, they can establish secure connections based on DIDs for enhanced authentication and trust in their interactions.

Construction Companies: Within construction companies, SSI can revolve around the management of VCs that store building-related information. These credentials can also integrate linked data and connect with IoT devices. This approach holds the potential to significantly improve data management practices and foster a more interconnected and efficient construction process.

To define the structural components of the SSI wallet, it was decided to use the Sustainable Building Profile (Figure 29):

1. Building information system (information about building and building elements, with integrated linked data such as IFC-to-LBD graphs)
2. Building sensors system (data from IoT devices)
3. Building management system (information about services, licenses, certifications, and insurances)

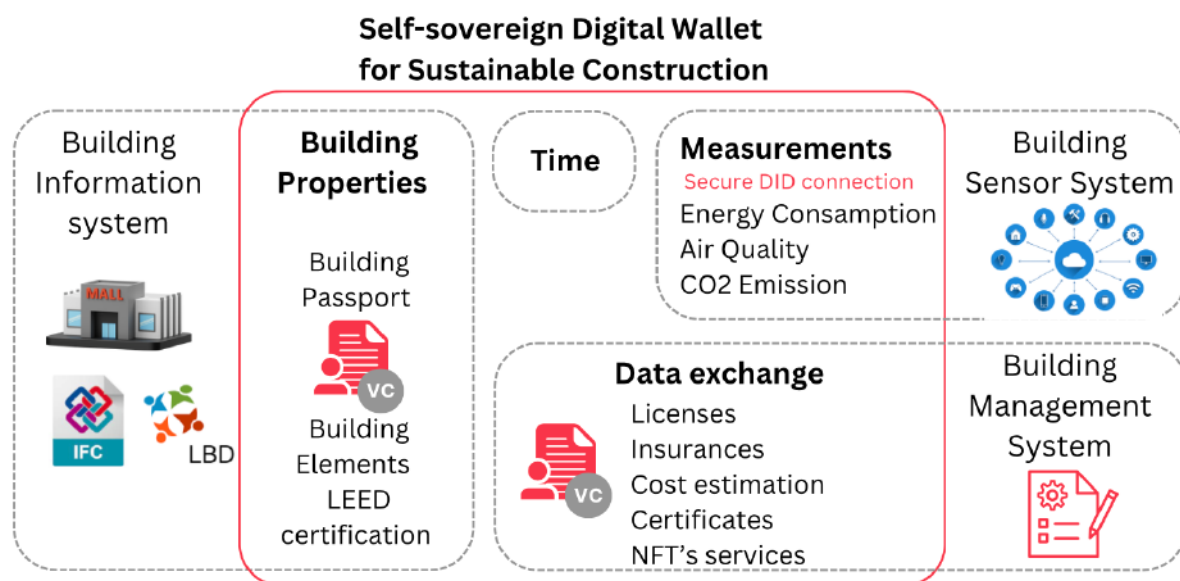


Figure 29: SSDW for Sustainable Construction

Considering these roles and components, it is advisable to emphasize three specific SSI implementation scenarios within the thesis:

1. **Enhancing Web Services Authentication via DIDs:** The first scenario focuses on bolstering web services authentication using DIDs, which are decentralized and secure identifiers. This approach enhances security, reduces identity theft risks, and grants users greater authority over their online identities.
2. **Establishing Secure Data Exchange Channels:** The second scenario revolves around the creation of secure data exchange channels. This is vital when sensitive information must be shared while maintaining data privacy and security. SSI ensures data exchanges are tamper-proof and verifiable, mitigating the risks of data breaches and unauthorized access.
3. **Securing VCs, NFTs, IoT data and DIDs Storage in Digital Wallets:** The third scenario underscores the importance of ensuring the secure storage of VCs within digital wallets. This safeguards critical information and offers users complete control over their VCs, guaranteeing privacy and security.

In these scenarios, the implementation of DIDs is integral to the SSI framework. DIDs serve as the foundation for secure identification and authentication, granting individuals and entities control over their digital identities and interactions. These decentralized identifiers, combined with digital wallets, enable stakeholders in the AEC industry to navigate a landscape where

security, privacy, and efficiency are paramount. With SSI and DIDs at the core, contractors and construction companies alike can embrace a new era of trust, connectivity, and innovation within their respective domains.

4.1 SSI Data Model

To describe a system proposal, it was decided to create a UML class diagram, which shows a connection between the SSI components SSI (Figure 30 – 33).

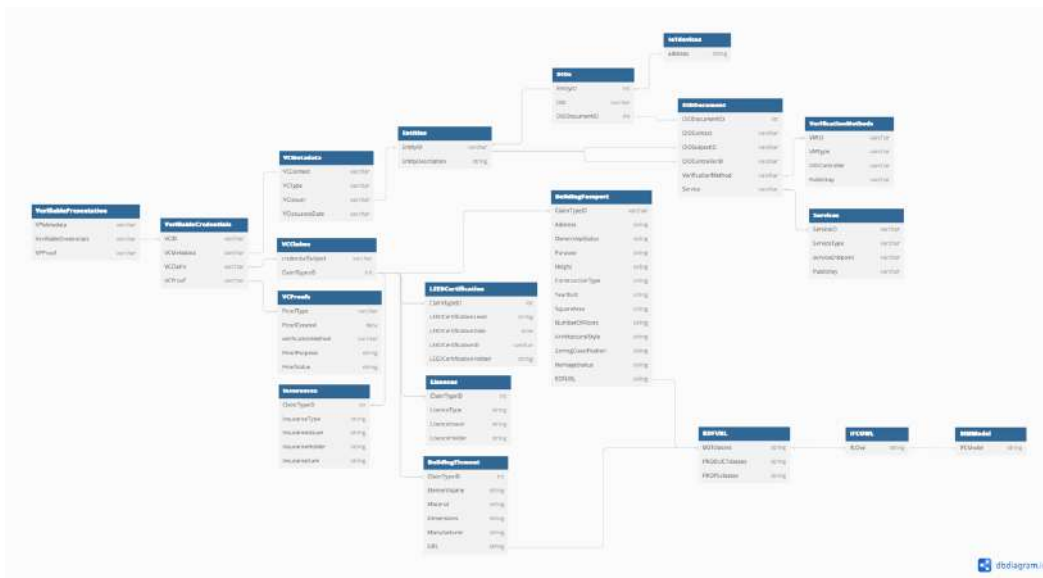


Figure 30: SSI Data model for a system proposal

This diagram was generated using <https://dbdiagram.io/>, a tool that assists in creating visual representations of database diagrams based on DBML (Database Markup Language) code. DBML is an open-source domain-specific language specifically crafted for defining and documenting database schemas and structures.

```

90 }
91
92 Table Licenses {
93   ClaimTypeID int
94   LicenseType string
95   LicenseIssuer string
96   LicenseHolder string
97 }
98
99 Table Insurances {
100   ClaimTypeID int
101   InsuranceType string
102   InsuranceIssuer string
103   InsuranceHolder string
104   InsuranceSum string
105 }
106
107 Ref: "DIDDocument", "VerificationMethod" < "VerificationMethods", "VMID"
108
109 Ref: "DIDDocument", "Service" < "Services", "ServiceID"
110
111 Ref: "VerifiableCredentials", "VCMetadata" - "VCMetadata", "VCContext"
112
113 Ref: "VerifiableCredentials", "VCClaim" < "VCClaims", "credentialSubject"
114
115 Ref: "VerifiablePresentation", "VerifiableCredentials" < "VerifiableCredentials", "VCID"
116
117 Ref: "VCClaims", "ClaimTypeID" < "LEEDCertification", "ClaimTypeID"
118
119 Ref: "VCClaims", "ClaimTypeID" < "BuildingPassport", "ClaimTypeID"

```

Figure 31: Example of visualization of data model diagrams from DBML code

It has two main parts: tables and relationships.

The figure shows DBML code for a table and its corresponding structure. On the left, the DBML code defines a table named 'VerifiablePresentation' with three columns: 'VPMetadata' (varchar), 'VerifiableCredentials' (varchar), and 'VPProof' (varchar). On the right, a diagram shows the 'VerifiablePresentation' table with its columns and data types: VPMetadata (varchar), VerifiableCredentials (varchar), and VPProof (varchar).

Figure 32: DBML code for tables

The figure shows DBML code for relationships between tables and a diagram illustrating these relationships. On the left, the DBML code lists several relationships, with one highlighted in a red box: 'Ref: "VCMetadata"."VCIssuer" - "Entities"."EntityID"'. On the right, a diagram shows two tables: 'VCMetadata' and 'Entities'. The 'VCMetadata' table has columns: VCContext (varchar), VCType (varchar), VCIssuer (varchar), and VCissuanceDate (varchar). The 'Entities' table has columns: EntityID (varchar) and EntityDescription (string). A red box highlights the 'VCIssuer' column in 'VCMetadata' and the 'EntityID' column in 'Entities', with a line connecting them to indicate a relationship.

Figure 33: DBML code for relationships between tables

This DBML code defines the schema for a relational database that could be used to store information related to DIDs, VCs, and other associated data in a structured manner. Below is a description of the main tables and their relationships:

1. **DIDs:** This table stores information about DIDs, including an entity identifier (EntityID), the DID itself, and a reference to the associated DID document.
2. **DIDDocument:** Contains details of DID documents, such as the DID context, DID subject, DID controller, verification methods, and services associated with the DID.
3. **VerificationMethods:** Stores information about verification methods used within DID documents, including the method ID, type, controller, and public key.
4. **Services:** Contains details about services referenced in DID documents, including the service ID, service type, service endpoint, and associated public key.
5. **VerifiableCredentials:** This table stores Verifiable Credentials, including the credential ID, metadata, claims, and proof information.
6. **VCMetadata:** Contains metadata related to Verifiable Credentials, such as context, type, issuer, and issuance date.
7. **VCClaims:** Stores information about claims within Verifiable Credentials, including the credential subject and reference to claim types.
8. **VCProofs:** Contains proof information for Verifiable Credentials, including proof type, creation date, verification method, proof purpose, and proof value.

9. **VerifiablePresentation:** Stores information about Verifiable Presentations, including metadata, references to Verifiable Credentials, and proof information.
10. **Entities:** Contains general information about entities, including an entity identifier and description.
11. **BuildingPassport:** This table stores data related to building passports, such as address, ownership status, purpose, height, construction type, year built, square area, number of floors, architectural style, zoning classification, and heritage status.
12. **LEEDCertification:** Stores information about LEED certifications, including certification level, certification date, certification ID, and certification holder.
13. **Licenses:** Contains details about licenses, including license type, issuer, and holder.
14. **Insurances:** Stores information about insurances, including insurance type, issuer, holder, and insurance sum.
15. **URL:** Stores information related to BOT classes, PRODUCT classes, PROPS classes.
16. **ifcOWL:** Stores data related to the IFCOWL.

The "Ref" lines at the end of the code represent relationships between tables, indicating how data in different tables is connected through foreign keys.

This schema is designed to support the storage and retrieval of information related to DIDs, VCs, entities, building data, certifications, licenses, and insurances in a structured and relational manner.

The DBML code presented in the GitHub repository.

4.2 Scenarios of SSI Implementation

For this particular use case, both the construction company (referred to as the appointing party) and the contractor (referred to as the lead appointed party) possess SSI Wallets. In this context, a construction company lists various services on the marketplace as Non-Fungible Tokens (NFTs). To obtain NFTs, contractors are required to demonstrate their competence by presenting their VCs, including work licenses, certificates, and other essential documentation. List of credentials is presented in section 4.5.

It was decided to utilize the IDP Kit and SSI Kit from walt.id. IDP Kit offers SSI- & NFT/SBT-based login. The SSI Kit provides a foundational identity infrastructure that can be applied to any use case across various industries. Its central services encompass (Figure 34):

1. Key Management: generating, signing, importing, exporting, and managing the life cycle of cryptographic keys.
2. DID Operations: registering, resolving, and managing the life cycle of DIDs, which are unique and self-sovereign identifiers.
3. VC, VP Operations: creating, issuing, presenting, and verifying verifiable credentials and presentations, which enable secure and trusted data sharing.

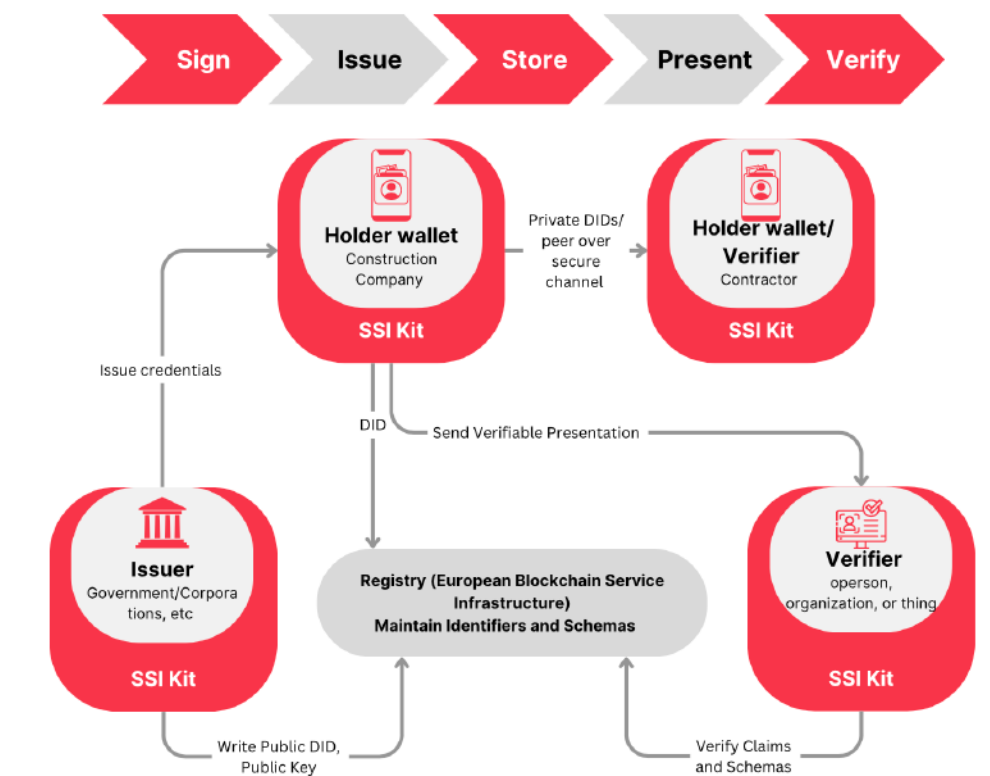


Figure 34: SSI Kit integration

4.2.1 Enhancing Web Services Authentication via DIDs.

The workflow for SSI implementation is visually represented in the accompanying Figure 35.

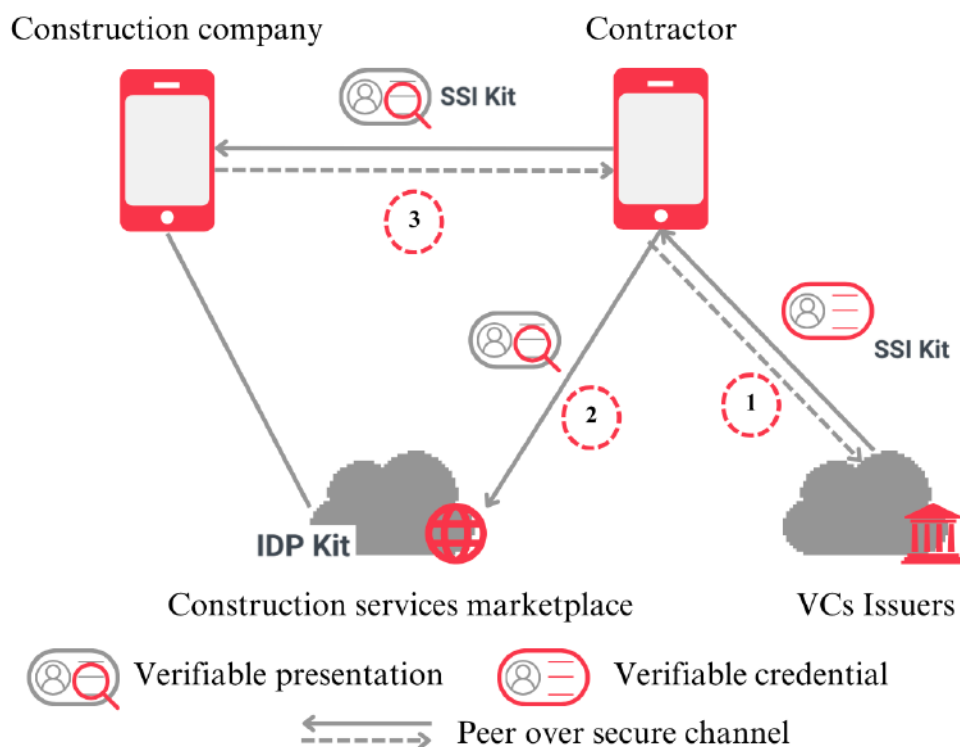


Figure 35. Scenario of SSI Implementation for getting access to marketplace and peer over secure channel

① The first step is Credential Request. The contractor initiates the process by connecting to issuers and requesting credentials. The contractor's edge agent guides them through the necessary steps to prove their identity to the issuer. Once the contractor fulfills the issuer's requirements, the credential is sent to the contractor's edge agent for storage.

② The second step involves gaining access to the NFT marketplace, which, for this scenario, incorporates the IDP Kit provided by walt.id. Here's how the process unfolds when employing SSI and verifiable credentials for information retrieval:

1. **Authentication Request:** The process begins with an authentication request made to the IDP Kit (walt.id). This request is intended to access the NFT marketplace.
2. **Credential Derivation:** The IDP Kit leverages SSI and verifiable credentials to derive the necessary credentials based on the authentication request. It then initiates a redirection to the user's SSI wallet, requesting a presentation of these required credentials. This interaction follows the OIDC/SIOPv2 presentation exchange protocol.
3. **SSI Wallet Response:** Upon receiving the presentation request, the user's SSI wallet responds by presenting the requested credentials.
4. **Verification and Compliance:** The IDP Kit verifies the response from the SSI wallet, including checking the signature, assessing the challenge, and ensuring compliance with

specific requirements. Additional verification policies, as outlined in the IDP Kit's configuration, may also be applied.

5. **Response Transformation:** Once the credential data has been successfully verified, the IDP Kit proceeds to transform this data into the response format that the application requires. This format can take the shape of standard claims (such as name and email) or a verifiable presentation containing the raw credential data shared by the user's SSI wallet.

The figure 36 illustrates an IDEF0 diagram depicting this workflow.

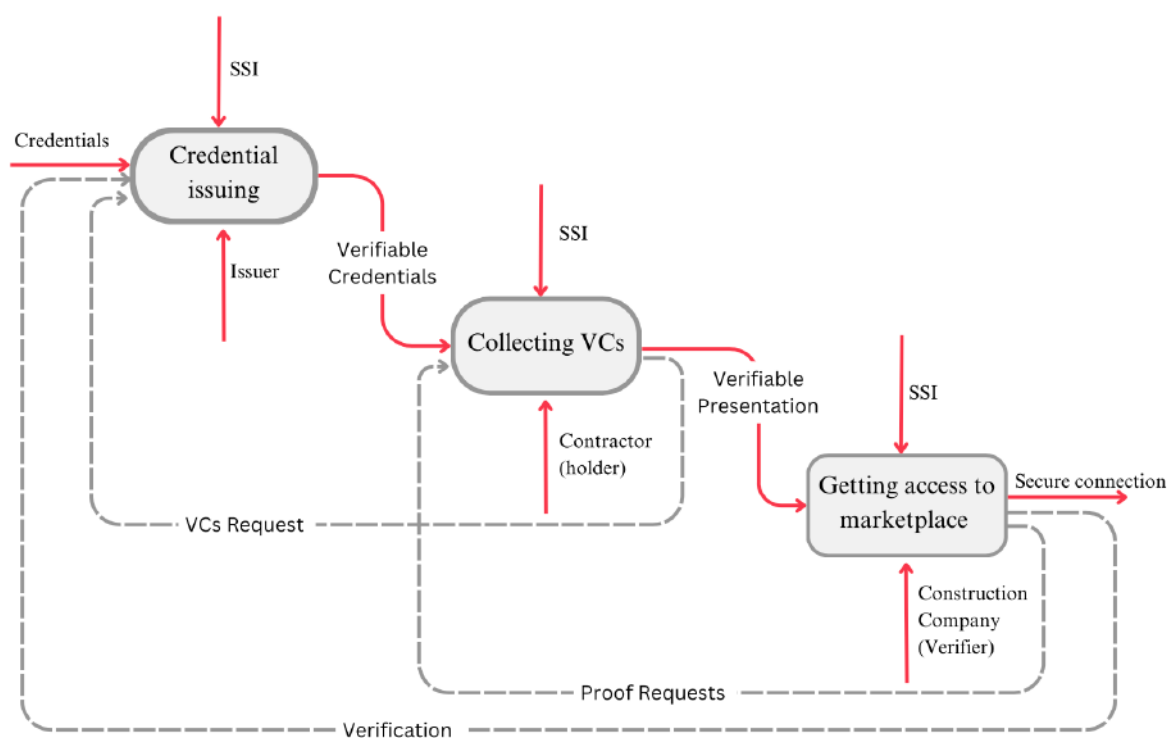


Figure 36: IDEF0 diagram depicting Scenario of SSI Implementation for getting access to marketplace

4.2.2 Establishing Secure Data Exchange Channels

This workflow can be enhanced by considering a scenario where the Contractor requests information from Construction company. In this case, the workflow is enhanced to include the exchange of VCs containing building-related information.

- 9 The third step is the connection between the construction company agent and the Contractor agent. The construction company receives the connection request and approves it. Their edge agent generates the necessary key pair, DID, and DID document for the connection response, which is sent back via the cloud agents to the contractor's edge agent, finalizing the connection.

4 The fourth step is VC Collection and Creation by Construction Company. In this use case, the Construction company takes on a dual role as both an issuer of VCs and a holder of a digital wallet. They meticulously prepare VCs containing standardized information about buildings and building elements. Additionally, the Construction company initiates requests for VCs from other relevant stakeholders.

5 The fifth step is Data exchange: Facilitated by a secure connection, the Contractor and Construction company can seamlessly request VCs that encompass comprehensive details about building (Figure 37).

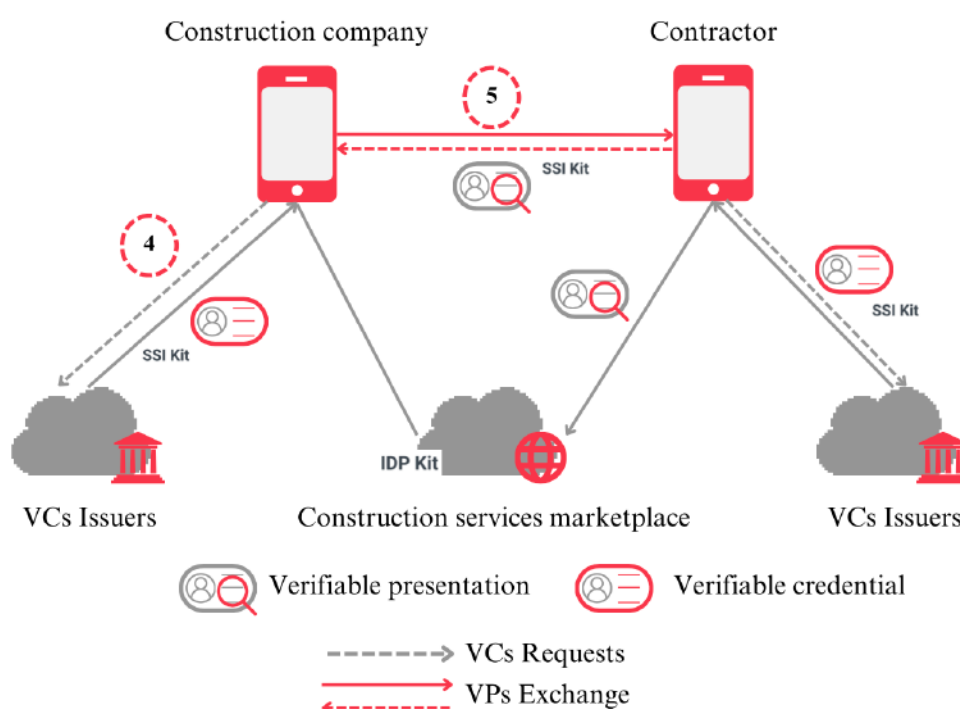


Figure 37: Scenario of SSI Implementation for Data exchange

That can be done because DIDs rely on asymmetric-key cryptography, also known as public-key cryptography. It employs a pair of keys: a public key and a secret (private) key. These keys are mathematically linked and used together. When one key alters a message, only the other key can revert the message to its original state.

The secret key must remain private, whereas the public key can be shared openly. Anyone can utilize a public key to encrypt a message that only someone with the secret key can decrypt. The private key, which is also termed the secret key, is typically used to compute the public

key. However, deriving the private key from the public key is not possible due to the unidirectional nature of the function involved.

Private keys are usually large, random numbers that are practically impervious to brute-force attacks. To encrypt a message using public-key cryptography, the recipient's public key is needed. This key transforms the message into ciphertext, which can only be converted back into the original message using the corresponding private key.

In the context of DIDs, the holder stores private keys for DIDs in their digital wallet, while the public keys for DIDs can be openly accessible. Figure 38 provides an example of the public and private keys linked to a DID using the Sovrin DID method.

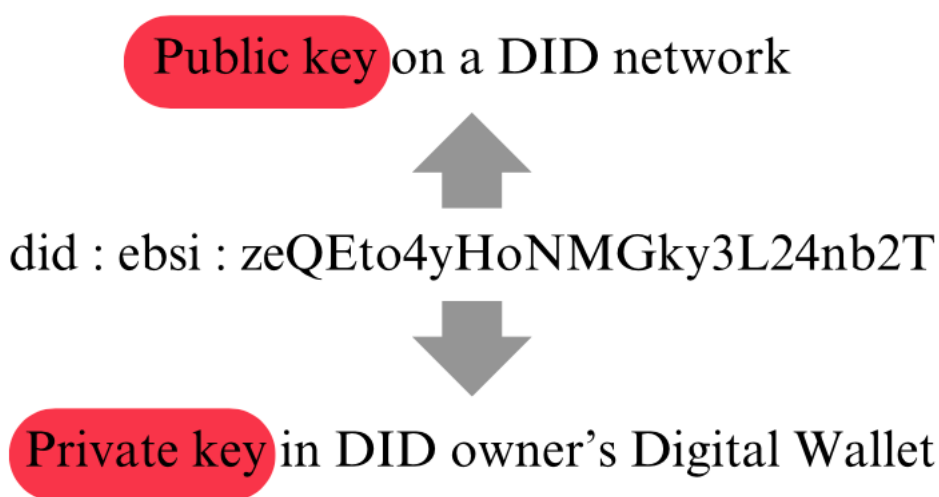


Figure 38: DID with a public and private key – Source: (Reed, Allen and Vogelsteller, no date)

The controller initially generates the public key-based identifier (DID) using the genesis public-private key pair. Afterward, the controller publishes the initial DID document, which includes the DID and the public key, as illustrated in figure 39.1.

Anyone who has access to the DID document can validate the cryptographic link between the DID and its associated public key, either by confirming the transaction address or by verifying the self-certifying identifier. When the controller decides to change the key pair, they generate an updated DID document and sign it using the previous private key, as illustrated in figure 39.2. Importantly, this process doesn't require human intervention; the controller can execute the transaction whenever they have control of the associated private key.

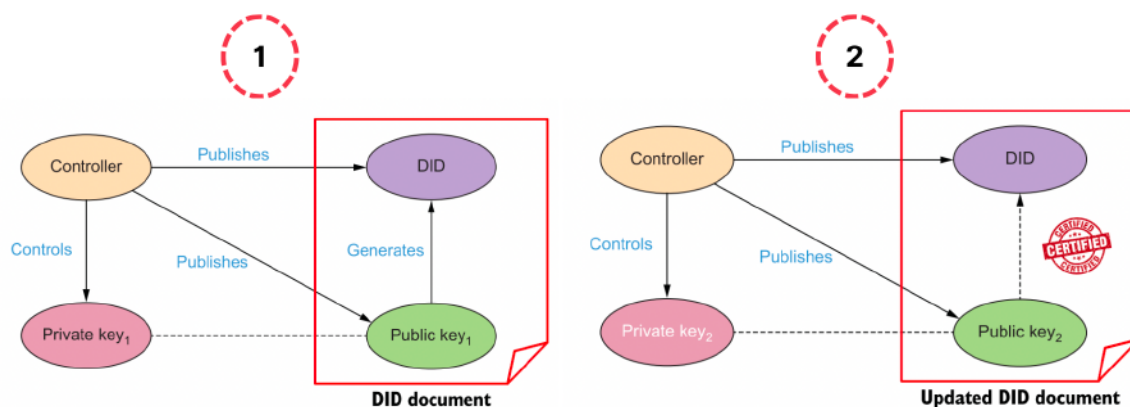


Figure 39: The PKI trust triangle includes a digital identifier for the controller – Source: (Reed, Allen and Vogelsteller, no date)

4.3 Securing VCs, NFTs, IoT data and DIDs Storage in Digital Wallets

4.3.1 GUI of Digital Wallet

The primary emphasis of this research endeavor centers around the development of a self-sovereign digital wallet, a critical component within the realm of decentralized identity and verifiable credentials. In pursuit of this objective, a user-friendly graphical user interface (GUI) has been meticulously crafted, encompassing fundamental functionalities essential for the efficient operation of this digital wallet. Digital Wallet views map is presented on the figure below.

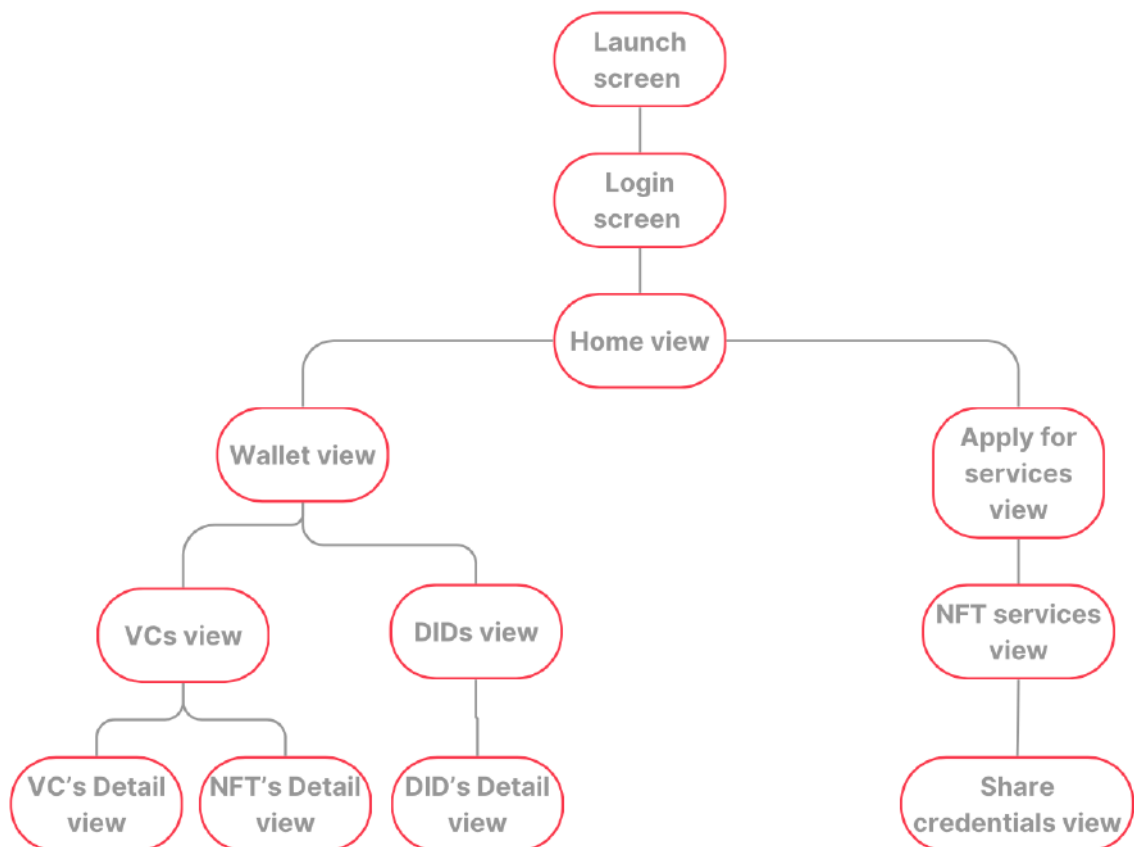


Figure 40: Digital wallet views map

Step 1 - The user initiates the process by pressing the app icon for the self-sovereign digital wallet on their smartphone. This action launches the application.

Step 2 - Launch Screen: upon launching the app, the user is greeted by the "Launch Screen". The launch screen serves as the initial point of entry into the self-sovereign digital wallet application. It is often designed to provide users with a visually appealing and welcoming experience. Key elements of the launch screen include:

1. **App Logo/Icon:** The wallet's logo or icon is prominently displayed at the center or top of the screen, reinforcing brand identity.
2. **Background Image:** A background image or pattern may be used to enhance the aesthetic appeal of the launch screen. This image could relate to the wallet's theme or branding.
3. **App Name:** The name of the digital wallet application is usually displayed, ensuring users immediately recognize the purpose of the app.

Step 3 - Login Screen: the login screen is where users authenticate themselves to gain access to their digital wallet and its contents. Key elements of the login screen include:

1. **Username/Email/Phone:** Users are required to enter their credentials, which can include a username, email address, or phone number. This information serves as their unique identifier.
2. **Password:** A secure password is necessary to protect the wallet's contents. Users must enter their password correctly to proceed(Figure 41).

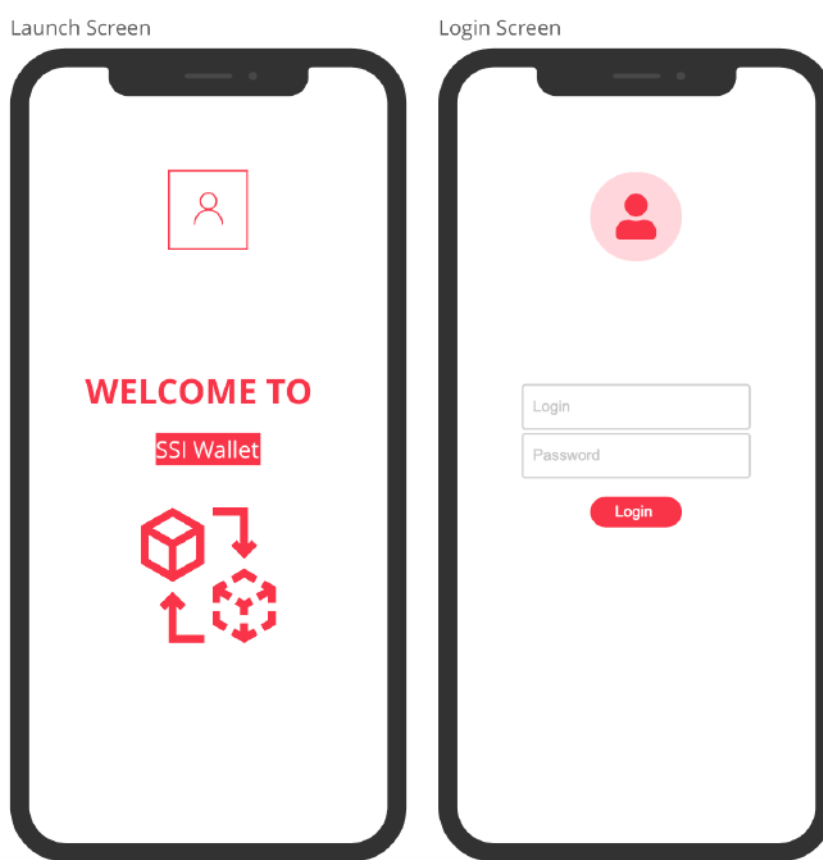


Figure 41: Launch and login screens

For the Contractor:

Step 4 - Home View Screen: The Home View Screen is the heart of the digital wallet application, offering users access to its core functionalities. Within this screen, users will find two primary functions that cater to the needs of contractors seeking to manage their professional identity and interact with construction companies:

1. **Wallet Section:** The "Wallet" section is a secure vault where users can access and manage their digital assets, including verifiable credentials, DIDs, and NFTs. Here's a breakdown of what this section offers (Figure 42):

- **Credentials:** Users can view, organize, and manage their collection of verifiable credentials within this subsection. These credentials may include licenses, certifications, qualifications, or any other attestations relevant to the contractor's profession.
- **NFTs:** This area is dedicated to managing NFTs that might represent ownership of unique digital assets related to services which the contractor has.
- **DIDs:** Contractors can review and maintain their unique DIDs, which are crucial for establishing trust and conducting secure interactions within the digital realm.

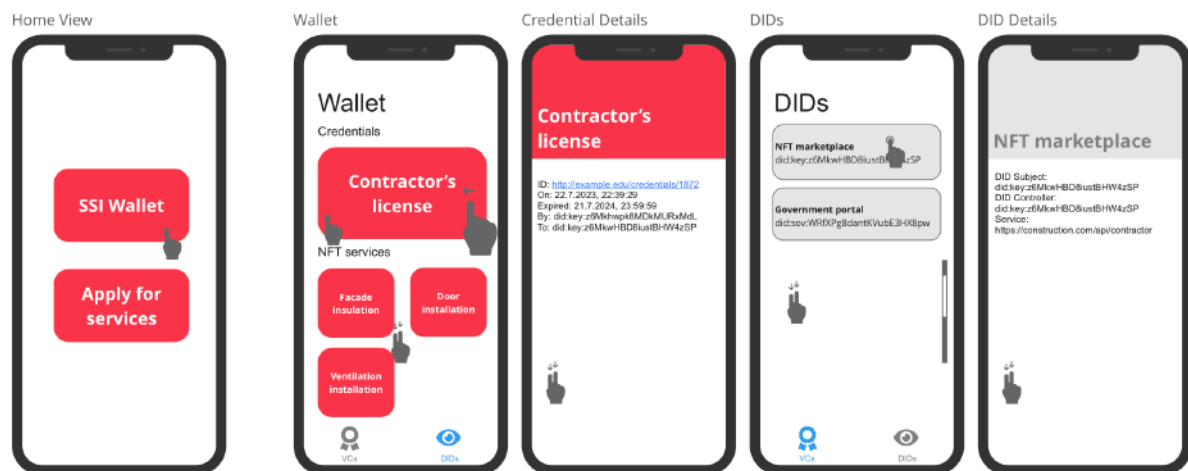


Figure 42: GUI for Home View and Wallet views of the Contractor's Wallet

2. **Apply to Service Section:** The "Apply to Service" section is where contractors can explore and engage with the services offered by construction companies (Figure 43). Here's how this section assists contractors in their interactions with construction companies:

- **Service Listings:** Contractors can browse through a catalog of construction services provided by various construction companies. Each service listing provides details about the offered service, such as its description, requirements, and any associated verifiable credentials (VCs) needed for application.
- **VC Sharing:** When a contractor finds a service they are interested in, they can initiate the application process directly from the digital wallet. This involves sharing

specific VCs with the construction company to prove their qualifications or eligibility for the service.

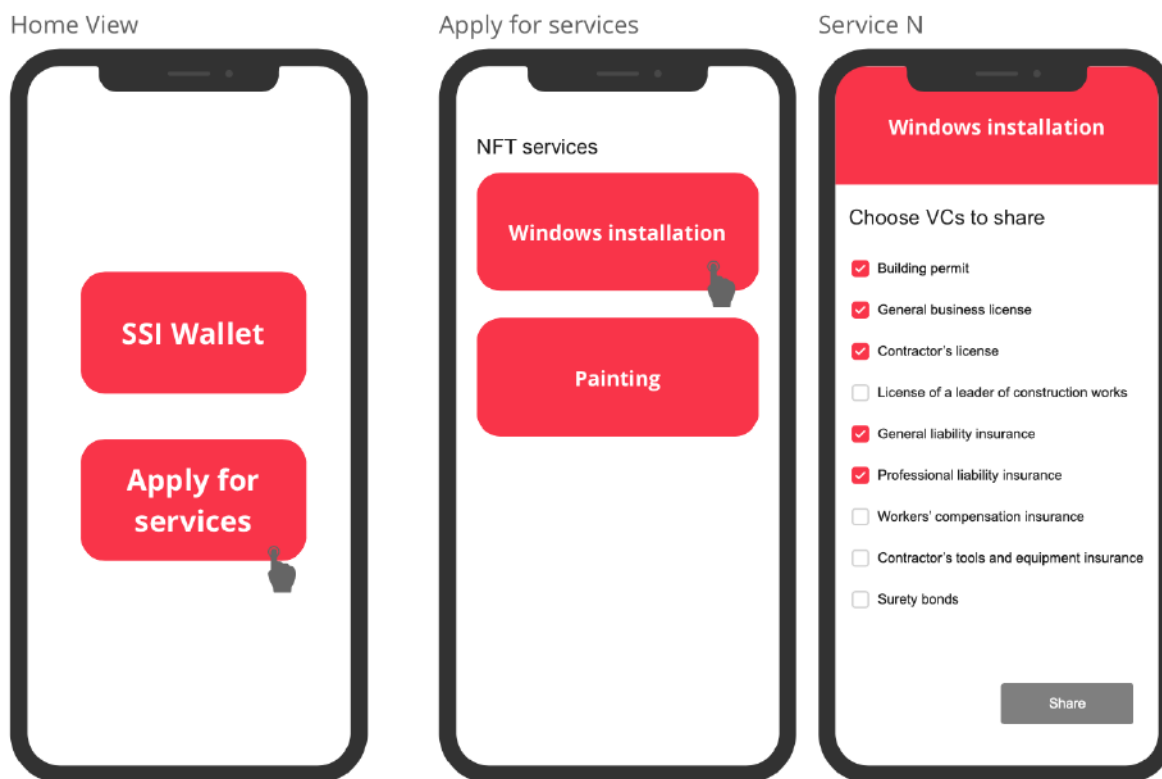


Figure 43: GUI of “Apply for services” views

For the Construction Company:

1. **Wallet Section:** The "Wallet" section is a secure vault where users can access and manage their digital assets, including verifiable credentials, DIDs, and NFTs. Here's a breakdown of what this section offers (Figure 44):
 - **Credentials:** Users can view, organize, and manage their collection of verifiable credentials within this subsection. These credentials may include licenses, certifications, qualifications, or any other attestations relevant to the contractor's profession.
 - **NFTs:** This area is dedicated to managing NFTs that might represent ownership of unique digital assets related to services which the Construction Company has.
 - **DIDs:** the Construction Company can review and maintain their unique DIDs, which are crucial for establishing trust and conducting secure interactions within the digital realm.

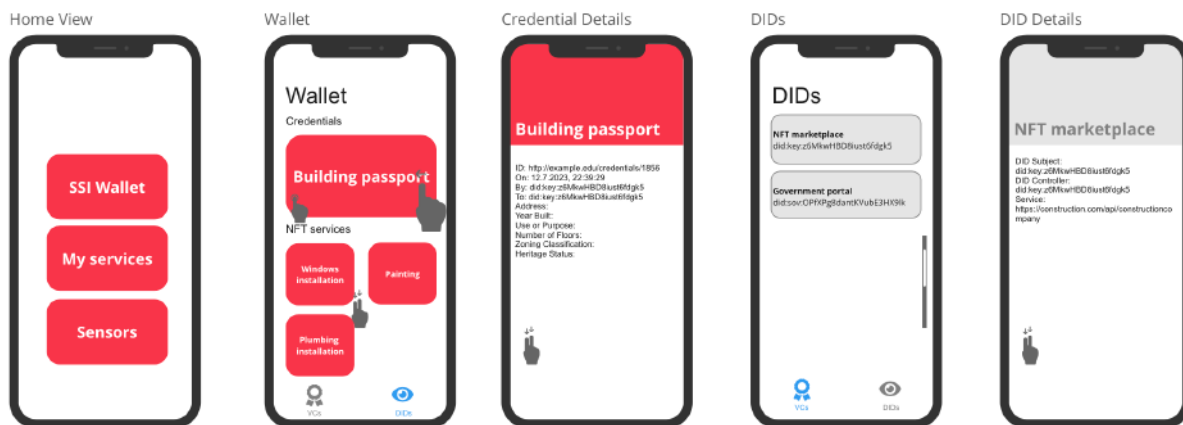


Figure 44: GUI for Home View and Wallet views of the Construction Company Wallet

2. **My Services Section:** The "My Services" section is where Construction Company can explore and engage with its services (Figure 45):

- **Service Listings:** Construction Company can browse through a catalog of services. Each service listing provides details about the offered service.
- **VC Sharing:** When a contractor finds a service they are interested in, they can ask for additional information directly from the digital wallet. This involves sharing specific VCs.

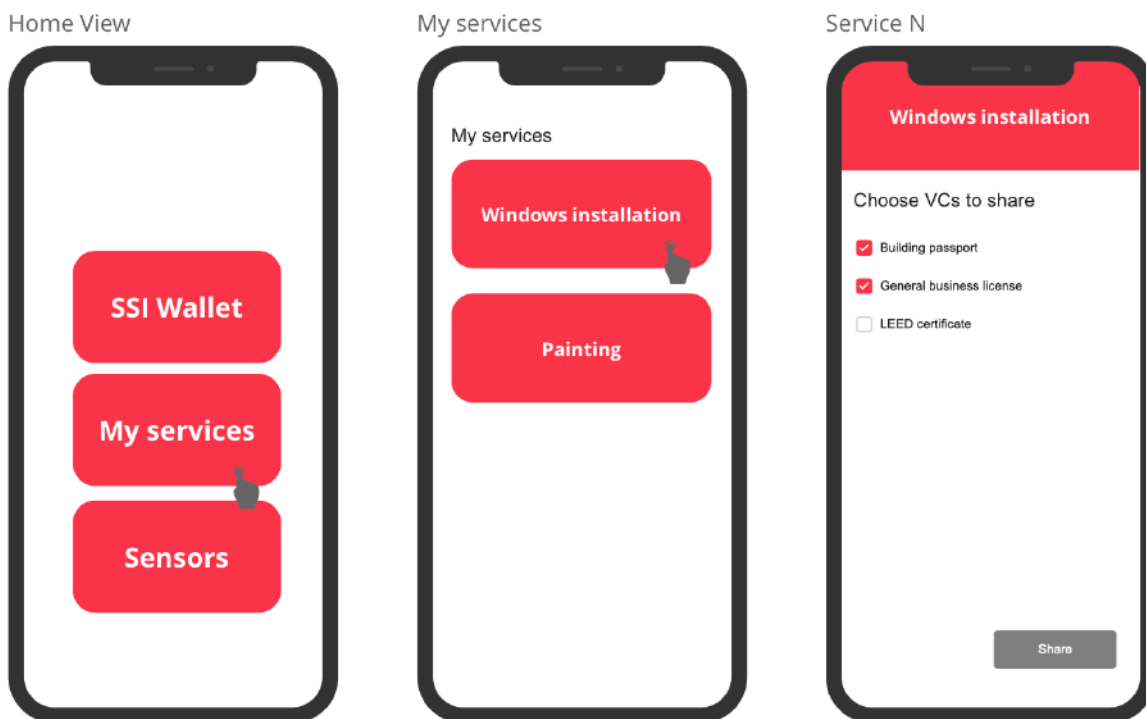
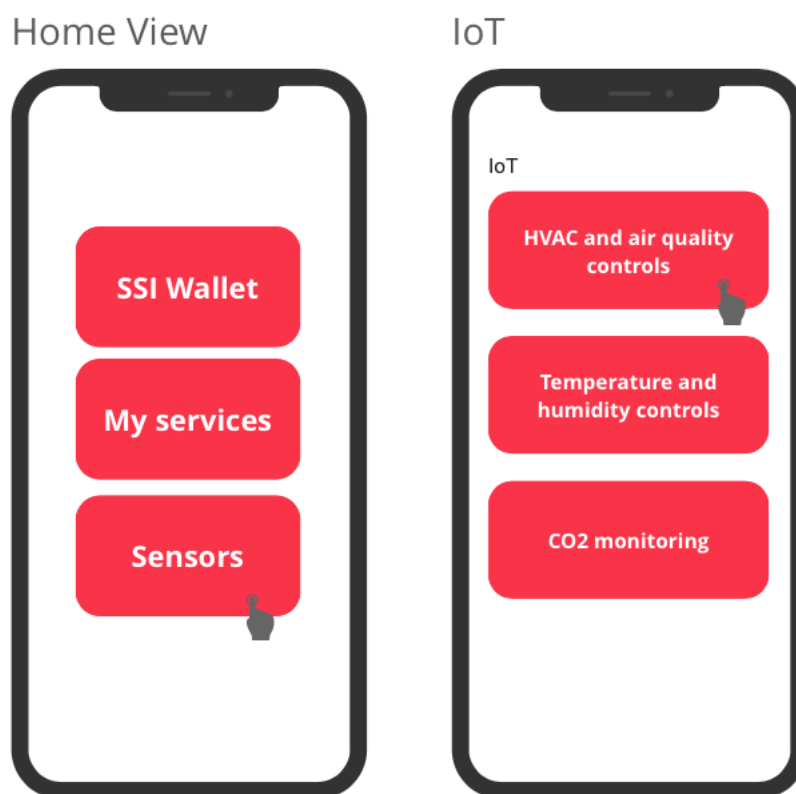


Figure 45: GUI of "My services" views

3. **Sensors Section:** The "Sensors" section provides information about measurements from IoT devices (Figure 46).



4.4 DIDs

In this use case we have 3 main roles and one 2 sub roles: Issuer, Contractor, Construction Company and Building and Services. To facilitate this, the SSI-Kit's REST API was launched on a local laptop using Docker. The Docker container was obtained directly from the Docker Hub, and the project was initiated via the following command in the Terminal: "docker run -p 7000-7004:7000-7004 -itv \$(pwd)/data:/app/data waltid/ssikit serve -b 0.0.0.0".

A folder named "data" was established within the current directory to serve as storage for various components such as VCs, DIDs, keys, and other essential data needed to enable full functionality (Figure 46).

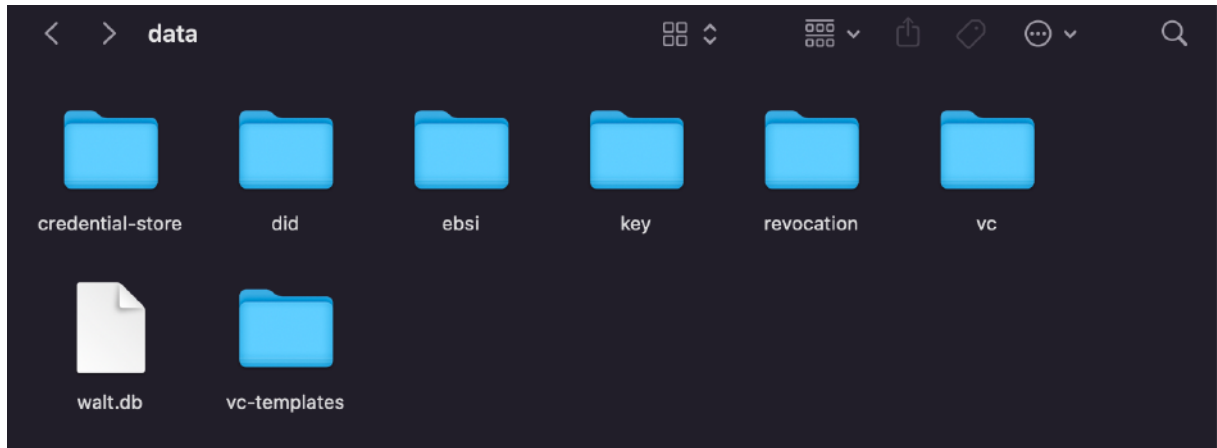


Figure 46: A storage for various components such as VCs, DIDs, keys, and other essential data

After successfully running the project, endpoints became accessible and ready for utilization (Figure 47).

```
walt.id Core API:      http://0.0.0.0:7000
walt.id Signatory API: http://0.0.0.0:7001
walt.id Custodian API: http://0.0.0.0:7002
walt.id Auditor API:  http://0.0.0.0:7003
walt.id ESSIF API:    http://0.0.0.0:7004
walt.id OIDC API:     http://0.0.0.0:7010
```

Figure 47: Exposed endpoints

DIDs were created through the SSI Kit API, with the EBSI DID Method selected (as shown in Figures 48-50).

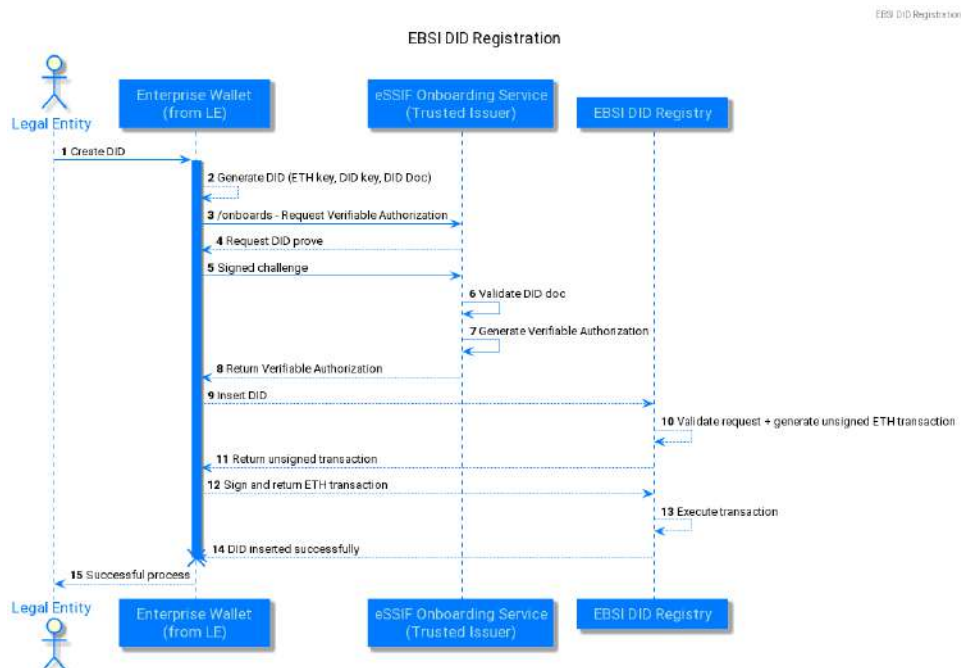


Figure 48: Creation and anchoring of a new DID on the EBSI ledger – Source: walt.id

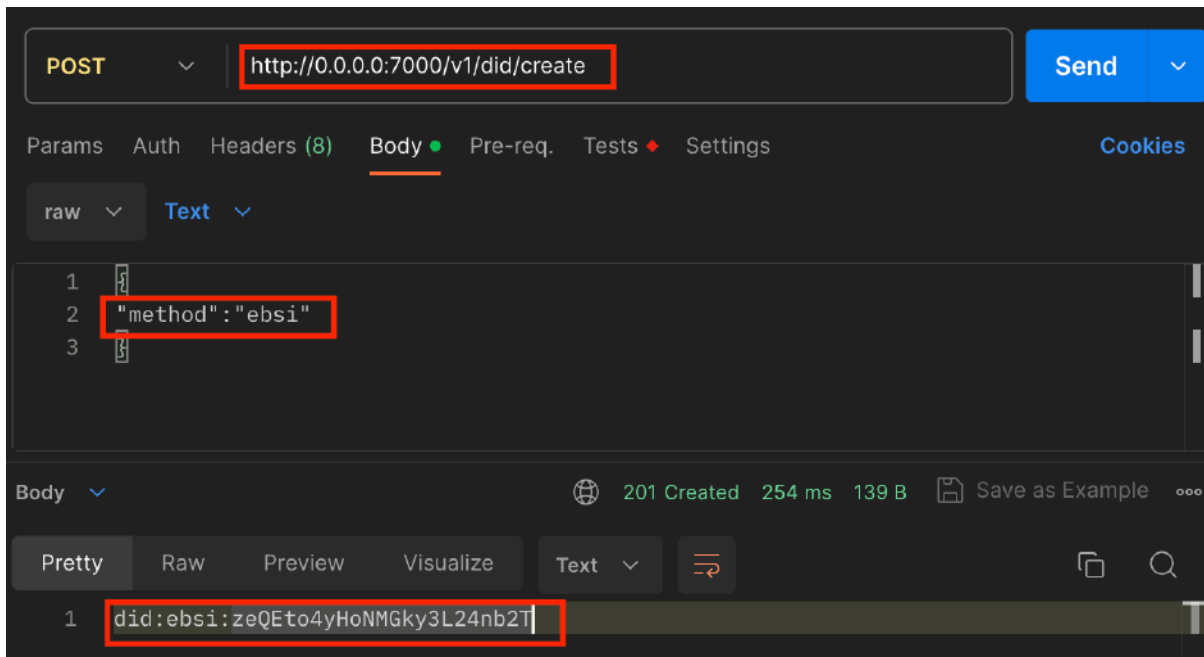


Figure 49: DID creation

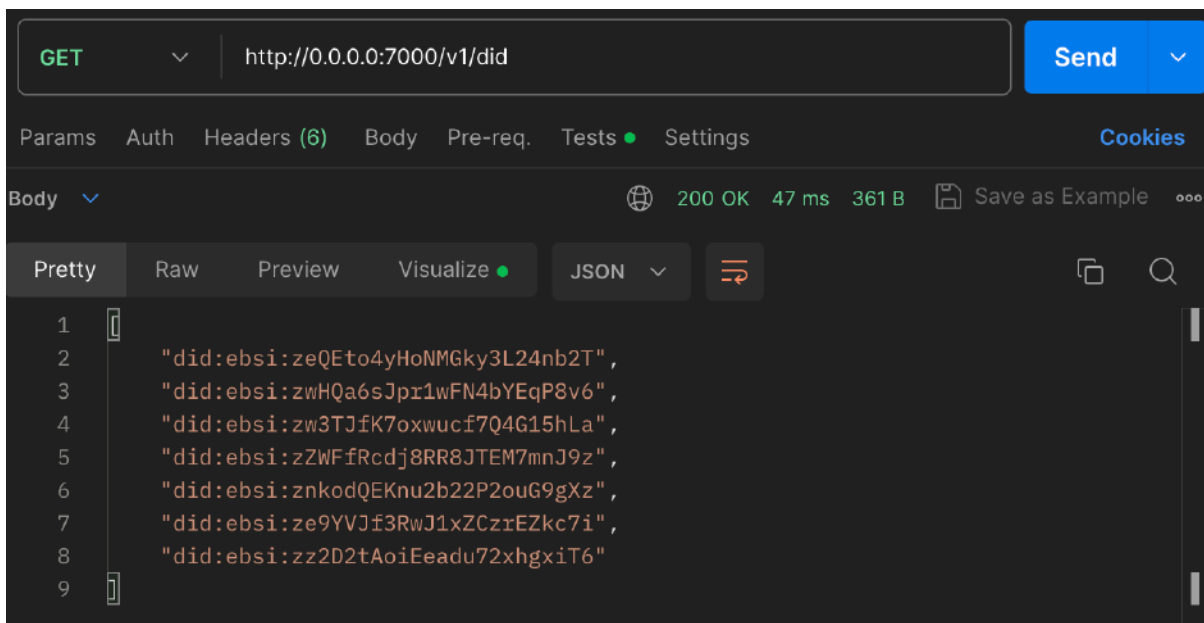


Figure 50: List of created DIDs

Table 1: DID key roles

Role	DID	DID Subject	DID Controller
Contractor	did:ebsi:zeQEto4yHoNMGky3L24nb2T	Contractor	Contractor
Services	did:ebsi:zwHQa6sJpr1wFN4bYEqP8v6	Services	Contractor
Construction Company	did:ebsi:zw3TJfK7oxwucf7Q4G15hLa	Construction Company	Construction Company

Building	did:ebsi:zZWFfRcdj8RR8JTEM7mnJ9z	Building	Construction Company
Issuer	did:iota:BnyZ9qUXrakyMNEaNmp6R 7K5PQxzDkfwnjYcuAoXyywR	Issuer	Issuer

The DID for a specific DID subject is represented by the **id** property within the DID document. The DID for a specific DID controller is represented by the **controller** property within the DID document.

Table 2: Basic DID properties

Property	Description
@context	Specifies the context for interpreting terms in the DID document.
id	Uniquely identifies the DID document.
controller	Identifies the entity (typically a DID) that controls the DID document.
verificationMethod	Contains the public keys and authentication mechanisms used for verification.

The Verification Method Properties related to the DID document:

Table 3: Verification Method Properties

Property	Description
id	A unique identifier for the verification method.
type	The type of the verification method, specifying its purpose or usage.
controller	Identifies the entity that controls the verification method.
publicKeyJwk	Represents the public key in JSON Web Key (JWK) format for cryptographic operations.

DID Document for did:ebsi:zeQEto4yHoNMGky3L24nb2T is presented in the figure below.

```

did%3Aebsi%3AzeQEto4yHoNMGky3L24nb2T
{
  "assertionMethod" : [
    "did:ebsi:zeQEto4yHoNMGky3L24nb2T#08c657cc44ac47d7bcf43ebf661c9d73"
  ],
  "authentication" : [
    "did:ebsi:zeQEto4yHoNMGky3L24nb2T#08c657cc44ac47d7bcf43ebf661c9d73"
  ],
  "@context" : "https://www.w3.org/ns/did/v1",
  "id" : "did:ebsi:zeQEto4yHoNMGky3L24nb2T",
  "verificationMethod" : [
    {
      "controller" : "did:ebsi:zeQEto4yHoNMGky3L24nb2T",
      "id" : "did:ebsi:zeQEto4yHoNMGky3L24nb2T#08c657cc44ac47d7bcf43ebf661c9d73",
      "publicKeyJwk" : {
        "alg" : "EdDSA",
        "crv" : "Ed25519",
        "kid" : "08c657cc44ac47d7bcf43ebf661c9d73",
        "kty" : "OKP",
        "use" : "sig",
        "x" : "EIBhxyN_pbU8f0l2HwKwUkv_IbtjzzUWHqMoswwfukM"
      },
      "type" : "Ed25519VerificationKey2019"
    }
  ]
}

```

Figure 51: DID resolution

4.5 Credentials

Verifiable Credentials for Construction Industry are presented in the table below.

Table 4. Verifiable Credentials for Construction Industry

Credential	Holder	Issuer	Description
Building passport	Construction company	Construction company	General information about building
LEED Certification	Construction company	Green Business Certification Inc.	Building reached or exceed certain environmental requirements
Building permit	Contractor/ Construction company	Governing authorities	Proof that the construction of a new or existing building can legally occur
General business license	Contractor	Governing authorities	Required by a city or county for the privilege of doing business in that jurisdiction.

Contractor's license	Contractor	Governing authorities	A type of occupational license that allows to legally engage in specific types of contracting work within a jurisdiction
A valid license of a leader of construction works	Contractor	Slovenian Chamber of Engineers – IZS Chamber of Architects (ZAPS) at Chamber of Craft Small Business of Slovenia (OZS)	A type of occupational license that allows to legally engage in specific types of contracting work within a jurisdiction
General liability insurance	Contractor	Governing authorities	Covering business if a visitor suffers an injury at a construction site or in the case of damage to a client's property.
Professional liability insurance	Contractor	Governing authorities	Covering the costs of a lawsuit if a client sues over a construction defect.
Workers' compensation insurance	Contractor	Governing authorities	Covering the costs of injured employees' medical bills and reimburse them for lost wages.
Contractor's tools and equipment insurance	Contractor	Governing authorities	Covering the costs of tools or machinery that have been lost, stolen, or damaged.
Surety bonds	Contractor	Governing authorities	A guarantee that the business will pay financial damages to

			government organizations if a third party sues them for the work.
--	--	--	---

Table 2 provides descriptions of the contents of basic VC's properties.

Table 5 Basic VC's properties

Property	Description
@context	Sequence of one or more URIs indicating the vocabularies used in constructing the VC.
type	List of URIs specifying the type of VC; the first type must be https://www.w3.org/2018/credentials/v1 .
issuer	URI uniquely identifies the issuer, which can point to a document describing the issuer, e.g., a DID document.
issuanceDate	Date and time when the credential becomes valid, expressed as an [XMLSCHEMA11-2] combined date-time.
credentialSubject	Contains claims made about the subject, including subject ID and asserted properties.
proof	Cryptographically proves issuance of the VC and its integrity since issuance.
expirationDate	ISO 8601 formatted date and time after which the VC is invalid.
credentialStatus	Provides verifier with VC's status (revoked, suspended, etc.) since issuance date.

Construction Company credentials properties are presented in the tables below.

Table 6: Construction Company claims

Property	Description
CompanyName	The official name of the construction company.
CompanyAddress	The physical address of the company's headquarters.
RegistrationNumber	The unique registration or identification number assigned to the company.
ContactEmail	The contact email address for the construction company.
ContactPhone	The contact phone number for the construction company.

```

{+} VCCCInformation > No Selection
1  {
2    "@context": [
3      "https://www.w3.org/2018/credentials/v1",
4      "https://www.example.com/construction-context/v1"
5    ],
6    "id": "urn:uuid:8e45fb16-90d8-4f61-b036-4efac0acbefd",
7    "type": ["VerifiableCredential", "ConstructionCompanyCredential"],
8    "issuer": "did:example:issuer",
9    "issuanceDate": "2023-08-25T14:17:00Z",
10   "expirationDate": "2024-08-25T14:17:00Z",
11   "credentialSubject": {
12     "CompanyName": "ConstructionCo Inc.",
13     "CompanyAddress": "123 Main Street, Cityville, State",
14     "RegistrationNumber": "1234567890",
15     "ContactEmail": "contact@constructionco.com",
16     "ContactPhone": "+1 (123) 456-7890"
17   }
18 }
    
```

Figure 52: Template for Construction Company VC

Table 7: Building passport claims

Property	Description
Height	The vertical measurement of the building from its base to its highest point.
Address	The physical location of the building, including street, city, state, and postal code.
Construction Type	The method or materials used in constructing the building.
Year Built	The year when the building was originally constructed.
Number of Floors	The total number of stories or levels in the building.
Architectural Style	The design or architectural style of the building.
Ownership Status	Indicates whether the building is owned, rented, or leased.
Purpose	The intended function or purpose of the building (e.g., residential, commercial).
Condition	The state of repair or maintenance (e.g., excellent, good, fair, poor).
Zoning Classification	The local government's zoning designation for property use.
Heritage Status	Designation as a heritage site or landmark for historical or architectural significance.

The template for the Building Passport VC is presented in the figure below.

```

VCCCBuildingPassportTemplate > No Selection
1 {
2   "@context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://example.com/context/construction-v1.jsonld"
5   ],
6   "id": "urn:uuid:1a3f79a0-6e0f-4d61-9f9e-6bb946c16d82",
7   "type": ["VerifiableCredential", "BuildingPassportCredential"],
8   "issuer": "did:example:issuer",
9   "issuanceDate": "2023-08-20T14:45:00Z",
10  "expirationDate": "2024-08-20T14:45:00Z",
11  "credentialSubject": {
12    "id": "did:example:building",
13    "address": "123 Main St, Anytown, CA 12345",
14    "height": "150 meters",
15    "constructionType": "Steel Frame",
16    "yearBuilt": "1995",
17    "numberOfFloors": "15",
18    "architecturalStyle": "Modern",
19    "ownershipStatus": "Owned",
20    "purpose": "Commercial",
21    "condition": "Excellent",
22    "zoningClassification": "Commercial",
23    "heritageStatus": "Not Designated"
24  },

```

Figure 53: Template for Building Passport VC

Table 8: LEED certification claims

Property	Description
Level	The level of LEED certification achieved for a project. This indicates the degree of sustainability and environmental performance attained.
Date	The date on which the LEED certification was awarded to the building or project.
ID	A unique identifier associated with the LEED certification. This identifier helps in tracking and referencing the specific certification for a project.
Issuer	The entity or organization that issued the LEED certification to the building or project.

The template for the LEED Certification VC is presented in the figure below.

```

{<code> VCCCLEEDCertificateTemplate > No Selection
1 {
2   "@context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://example.com/context/leed-v1.jsonld"
5   ],
6   "id": "urn:uuid:345e6d5e-98a1-4f97-babc-ae6a3bc6c951",
7   "type": ["VerifiableCredential", "LEEDCertificationCredential"],
8   "issuer": "did:example:issuer",
9   "issuanceDate": "2023-08-25T10:15:00Z",
10  "expirationDate": "2024-08-25T10:15:00Z",
11  "credentialSubject": {
12    "id": "did:example:buildingdid",
13    "claims": {
14      "Level": "Platinum",
15      "Date": "2023-08-20",
16      "ID": "LEED123456",
17      "Issuer": "Green Building Council"
18    }
19  }
20 }
    
```

Figure 54: Template for LEED Certification VC

Table 9: Building elements claims

Property	Description
Element Name	The name or label for the specific building element, such as "Roof," "Walls," "Windows," etc.
Material	The primary material used in the construction of the building element, which can include options like "Concrete," "Wood," "Glass," etc.
Dimensions	The physical dimensions or size specifications of the building element, which may include measurements like length, width, and height.
Sustainability	Details about the sustainability characteristics of the building element, such as whether it is recycled, recyclable, or made from renewable resources.
Manufacturer	The name of the manufacturer or supplier of the building element, which can be important for sourcing and warranty purposes.
Fire Rating	The fire rating or fire resistance level of the building element, indicating its ability to withstand fire for a specified duration.
URL	URL to RDF graph

The template for the Building Elements VC is presented in the figure below.

```

VCCCBuildingElementsTemplate > No Selection
1  {
2    "@context": [
3      "https://www.w3.org/2018/credentials/v1",
4      "https://example.com/context/building-elements-v1.jsonld"
5    ],
6    "id": "urn:uuid:7893f2d7-1a85-43c1-8b81-61b79bb674c1",
7    "type": ["VerifiableCredential", "BuildingElementsCredential"],
8    "issuer": "did:example:issuer",
9    "issuanceDate": "2023-08-26T14:30:00Z",
10   "expirationDate": "2024-08-26T14:30:00Z",
11   "credentialSubject": {
12     "id": "did:example:elementdid",
13     "claims": {
14       "ElementName": "Roof",
15       "Material": "Concrete",
16       "Dimensions": "10m x 5m x 0.2m",
17       "Sustainability": "Recyclable",
18       "Manufacturer": "Acme Building Supplies",
19       "FireRating": "Class A"
20     }
21   }

```

Figure 55: Template for Building Elements VC

Contractor credentials claims are presented in the tables below.

Table 10: Contractor Information claims

Property	Description
CompanyName	The official name of the construction company.
CompanyAddress	The physical address of the company's headquarters.
RegistrationNumber	The unique registration or identification number assigned to the company.
ContactEmail	The contact email address for the construction company.
ContactPhone	The contact phone number for the construction company.

```

{cc} VCCInformation > No Selection
1  {
2    "@context": [
3      "https://www.w3.org/2018/credentials/v1",
4      "https://www.example.com/contractor-context/v1"
5    ],
6    "id": "urn:uuid:8e45fb16-90d8-4f61-b036-4efac0acbafd",
7    "type": ["VerifiableCredential", "ContractorCredential"],
8    "issuer": "did:example:issuer",
9    "issuanceDate": "2023-08-25T14:17:00Z",
10   "expirationDate": "2024-08-25T14:17:00Z",
11   "credentialSubject": {
12     "CompanyName": "Co Inc.",
13     "CompanyAddress": "123 Main Street, Cityville, State",
14     "RegistrationNumber": "1234567890",
15     "ContactEmail": "contact@co.com",
16     "ContactPhone": "+1 (123) 456-7890"
17   }
18 }
    
```

Figure 56: Template for Contractor VC

Table 11: Licenses claims

Property	Description
License Number	A unique identifier assigned to the contractor's license.
License Type	The category or type of contractor license, indicating the specific trade or specialization, such as electrical, plumbing, general contracting, etc.
Issuing Authority	The government agency or organization responsible for issuing and regulating contractor licenses.
License Holder	The name of the individual or entity that holds the contractor license.
Scope of Work	Details about the specific scope of work or services that the contractor is authorized to perform under the license.
Geographic Area	The geographic area or jurisdiction where the contractor license is valid and applicable.
Insurance Coverage	Information regarding the contractor's insurance coverage, including liability and worker's compensation coverage.

The template for the Licenses VC is presented in the figure below.

```

{**} VCCLicenseTemplate > No Selection
1  {
2    "@context": [
3      "https://www.w3.org/ns/credentials/v2",
4      "https://www.w3.org/ns/credentials/examples/v2"
5    ],
6    "id": "http://example.gov/credentials/3732",
7    "type": ["VerifiableCredential", "ContractorCredential"],
8    "issuer": "did:example:issuer",
9    "issuanceDate": "2023-08-15T12:00:00Z",
10   "expirationDate": "2025-08-15T12:00:00Z",
11   "credentialSubject": {
12     "id": "did:example:contractor123",
13     "licenseNumber": "CL123456",
14     "licenseType": "General Contracting",
15     "issuingAuthority": "State Construction Board",
16     "licenseHolder": "John Doe",
17     "scopeOfWork": "Residential and Commercial Construction",
18     "geographicArea": "State of Example",
19     "insuranceCoverage": {
20       "liabilityCoverage": "Up to $1,000,000",
21       "workersCompensation": "Fully Covered"
22     }
23   }

```

Figure 57: Template for Licenses VC

Table 12: Insurance claims

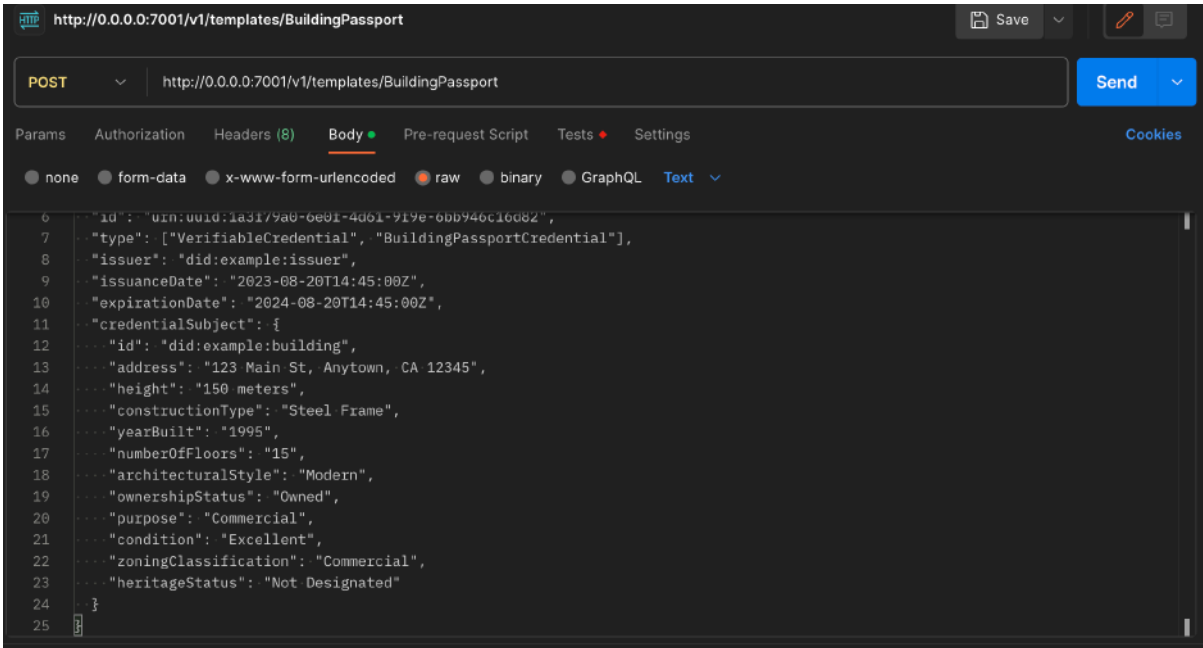
Property	Description
Insurance Type	The category or type of insurance, specifying the coverage provided, such as liability insurance, worker's compensation, or other types of insurance relevant to the construction industry.
Insurance Issuer	The name of the insurance company or provider that issued the insurance policy to the contractor.
Insurance Holder	The name of the individual or entity that holds the insurance policy, typically the contractor or their business entity.
Coverage Amount	The monetary limit of coverage provided by the insurance policy, indicating the maximum amount that can be claimed in case of a covered incident.
Policy Effective Date	The date when the insurance policy becomes effective and coverage begins.
Policy Expiration Date	The date when the insurance policy is set to expire, requiring renewal to maintain coverage.
Coverage Details	Specific details about what is covered by the insurance policy, including any exceptions or limitations.

The template for the Insurance VC is presented in the figure below.

```
{se} VCCInsuranceTemplate > No Selection
1  {
2    "@context": [
3      "https://www.w3.org/2018/credentials/v1",
4      "https://schema.org"
5    ],
6    "type": ["VerifiableCredential", "ContractorInsuranceCredential"],
7    "issuer": {
8      "id": "did:example:issuer123",
9      "name": "Example Insurance Company"
10   },
11   "issuanceDate": "2023-08-15T14:30:00Z",
12   "expirationDate": "2024-08-15T14:30:00Z",
13   "credentialSubject": {
14     "id": "did:example:contractor456",
15     "type": "Contractor",
16     "insuranceType": "Liability Insurance",
17     "insuranceIssuer": "Example Insurance Company",
18     "insuranceHolder": "John Contractor",
19     "coverageAmount": "$1,000,000",
20     "policyEffectiveDate": "2023-08-15",
21     "policyExpirationDate": "2024-08-15",
22     "coverageDetails": "Covers general liability claims for construction projects."
23   }
24 }
```

Figure 58: Template for Licenses VC

These templates were added to SSI Kit using endpoint <http://0.0.0.0:7001/v1/templates> (Figures 59-60).



```
http://0.0.0.0:7001/v1/templates/BuildingPassport
POST http://0.0.0.0:7001/v1/templates/BuildingPassport
Body
none form-data x-www-form-urlencoded raw binary GraphQL Text
6   "id": "urn:uuid:1a3179a0-6e01-4d61-919e-6bb946c16d82",
7   "type": ["VerifiableCredential", "BuildingPassportCredential"],
8   "issuer": "did:example:issuer",
9   "issuanceDate": "2023-08-20T14:45:00Z",
10  "expirationDate": "2024-08-20T14:45:00Z",
11  "credentialSubject": {
12    "id": "did:example:building",
13    "address": "123 Main St, Anytown, CA 12345",
14    "height": "150 meters",
15    "constructionType": "Steel Frame",
16    "yearBuilt": "1995",
17    "numberOfFloors": "15",
18    "architecturalStyle": "Modern",
19    "ownershipStatus": "Owned",
20    "purpose": "Commercial",
21    "condition": "Excellent",
22    "zoningClassification": "Commercial",
23    "heritageStatus": "Not Designated"
24  }
25 }
```

Figure 59: Template addition with SSI Kit API

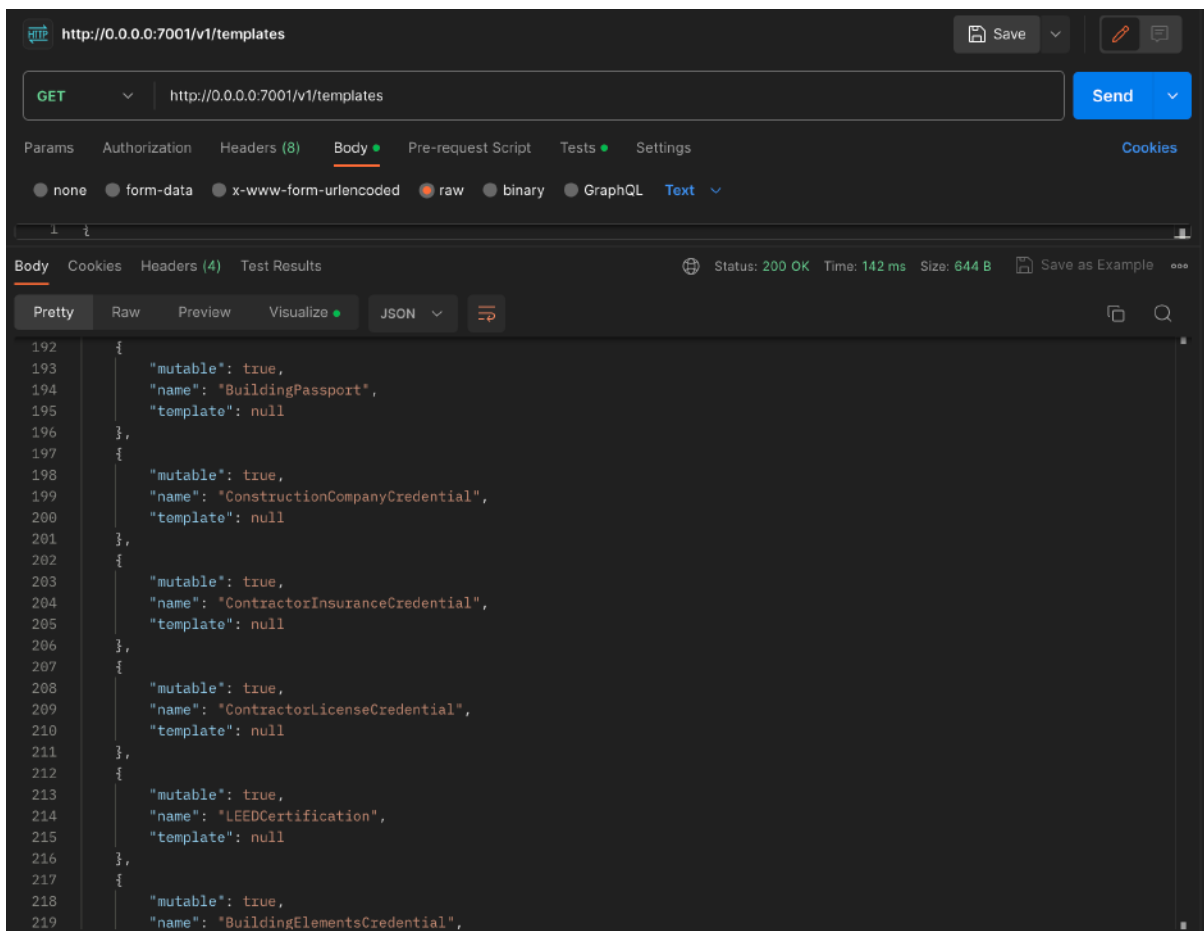


Figure 60: VC Templates with SSI Kit API

The next step involves issuing credentials to both the Construction Company and Contractor. To accomplish this, the following endpoint: <http://0.0.0.0:7001/v1/templates> was utilized (Figures 61-62).

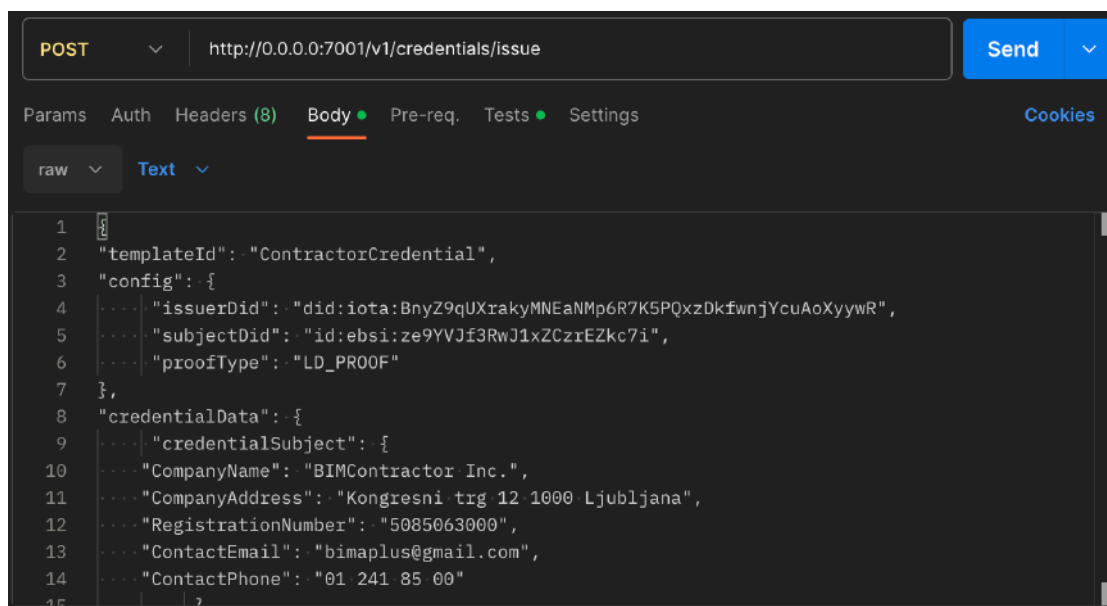


Figure 61: VC issuance with SSI Kit API

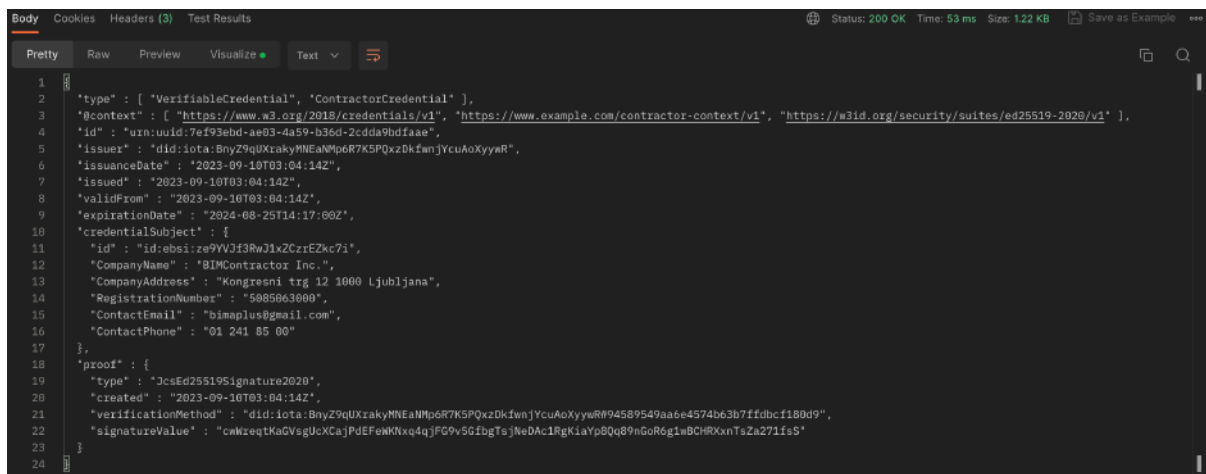


Figure 62: VC for Contractor

4.6 IFC-to-LBD

By employing the ifcOWL ontology, it becomes possible to represent building-related information using cutting-edge web technologies, specifically those associated with the semantic web and linked data. This approach transforms IFC data into a structured format known as RDF. Within this graph model, and thanks to the underlying web technology stack, building data can be seamlessly connected to a wide array of other data types. This includes materials data, GIS data, manufacturer data, sensor data, classification schemas, social data, and various others. The outcome is a dynamic web of interconnected building data, opening up significant opportunities for improved data management and enhanced data exchange capabilities, not only within the construction industry but also extending to broader applications. To integrate linked data, it is suggested to use IFC-to-LBD export which is described in section 2.1.3 (Figure 63).

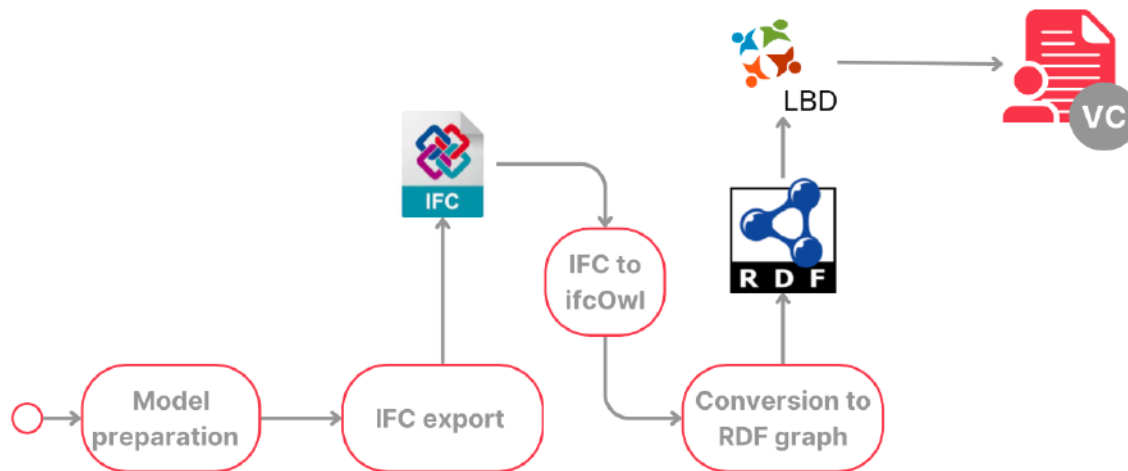


Figure 63: IFC-to-LBD

The IFC-to-LBD converter was employed for this case study. This open-source project is implemented in Java using the widely recognized Jena framework and is accessible on GitHub. The converter is designed to process IFC files from all actively utilized IFC schemas. It offers the flexibility to convert an IFC building model into a single RDF file that combines all the chosen LBD Abox modules (BOT, PROPS, and/or PRODUCT)(Janowicz *et al.*, 2020), or alternatively, into multiple separate RDF files based on the selected LBD module. The output can also be represented in the form of a JSON file, and the most suitable output format for this case study would be determined based on the specific requirements and objectives of the study(Bonduel *et al.*, 2018b).

The IFC-to-LBD converter was launch using Docker.

```
docker pull jyrkioraskari/ifc2lbdopenapi:latest
docker container run -it --publish 8081:8080 jyrkioraskari/ifc2lbdopenapi
```

Figure 64 IFC-to-LBD converter start

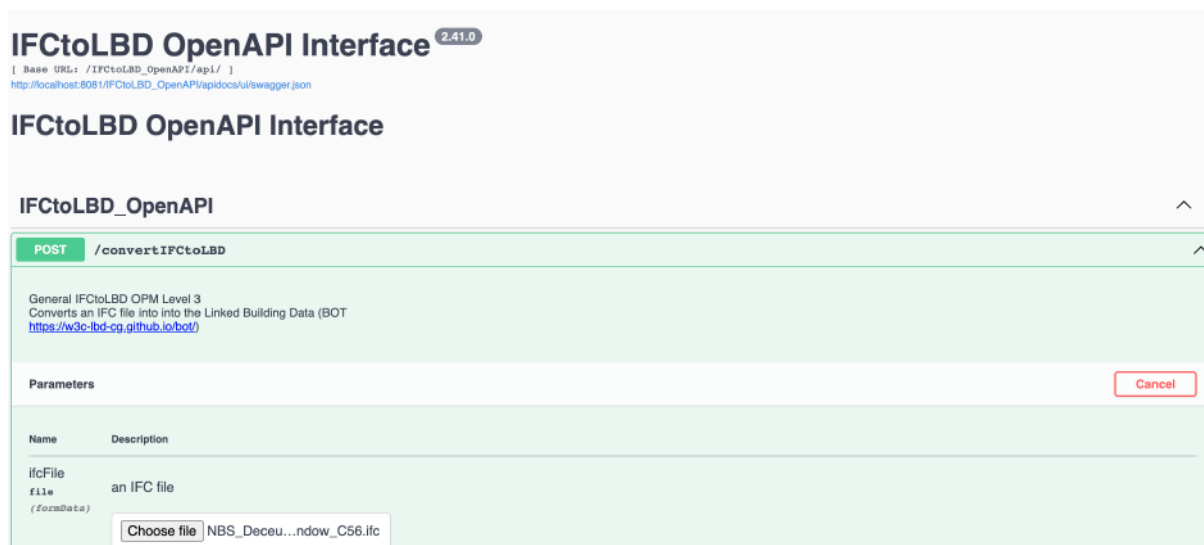


Figure 65: IFC-to-LBD converter interface

It was determined to utilize the IFC-to-LBD converter for processing Windows IFC files. The JSON file output resulting from this process is presented in the figure below.

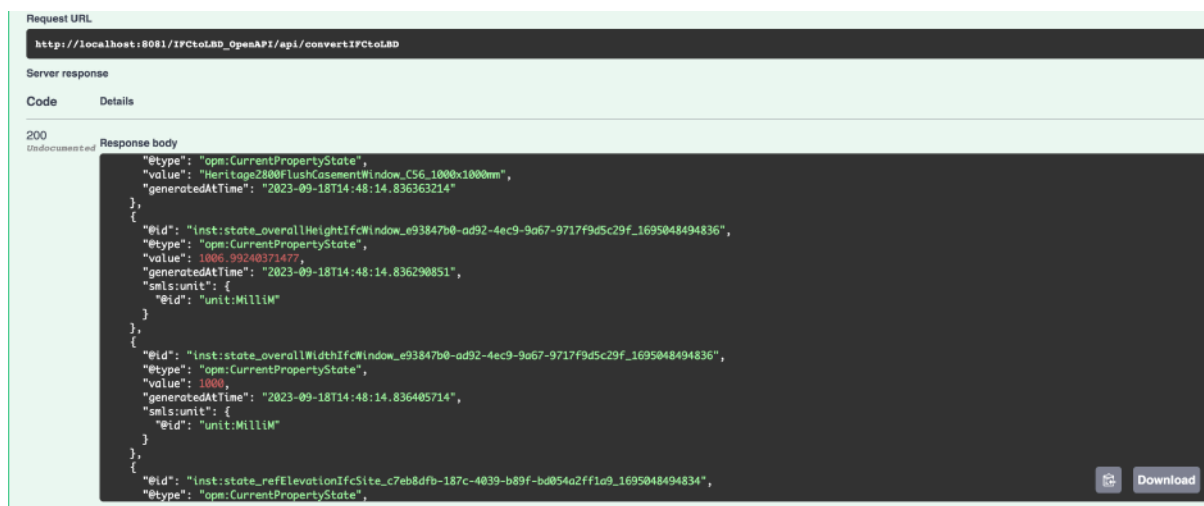


Figure 66: JSON representation of the IFCtoLBD transfer

This JSON file, which contains structured data representing building information, can be queried, and seamlessly integrated into VCs. By integrating this JSON data into VCs, it becomes a valuable source of verifiable and trusted information within a decentralized identity ecosystem. Users can retrieve specific data points or subsets of information from the JSON file and include them as claims within their VCs.

4.7 Implementation of a Digital Wallet with SwiftUI

Demo version of the digital wallet was developed using Swift UI.

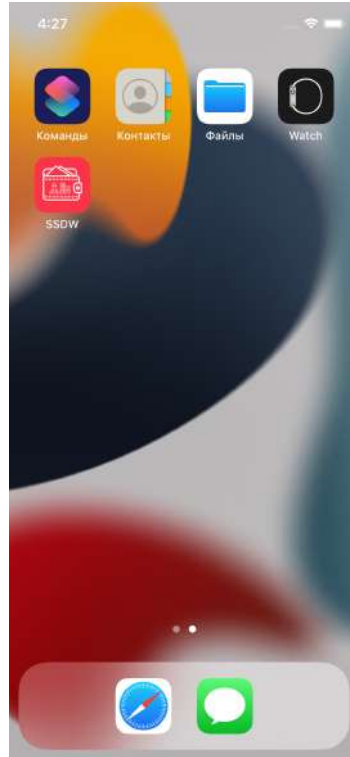


Figure 67: The app icon

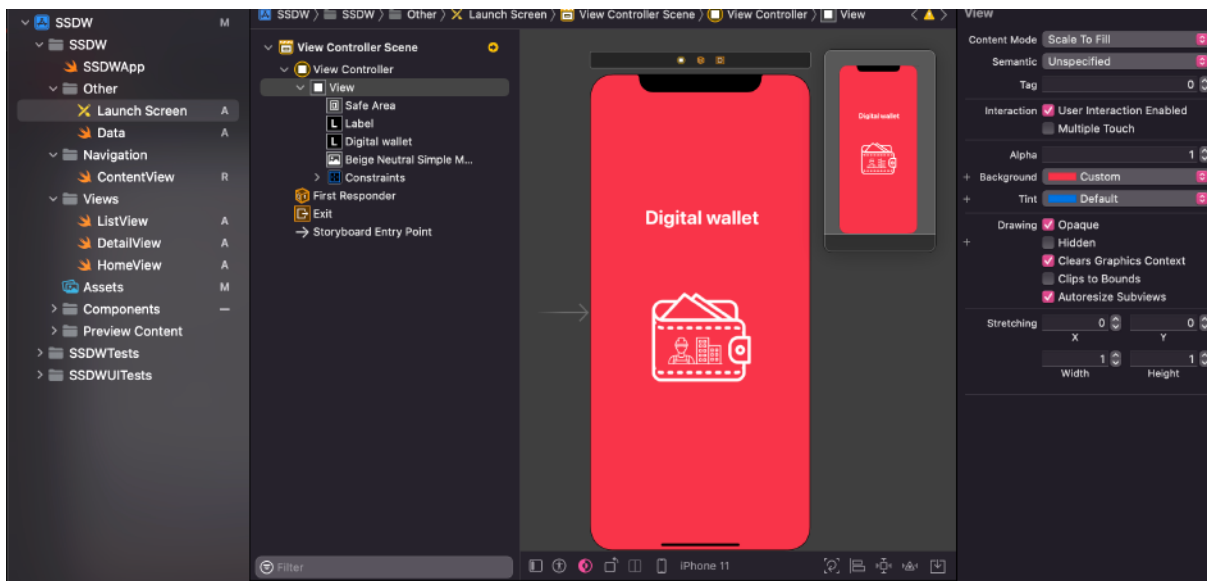


Figure 68: The Launch Screen

The first option of the SSDW is for the Contractor.

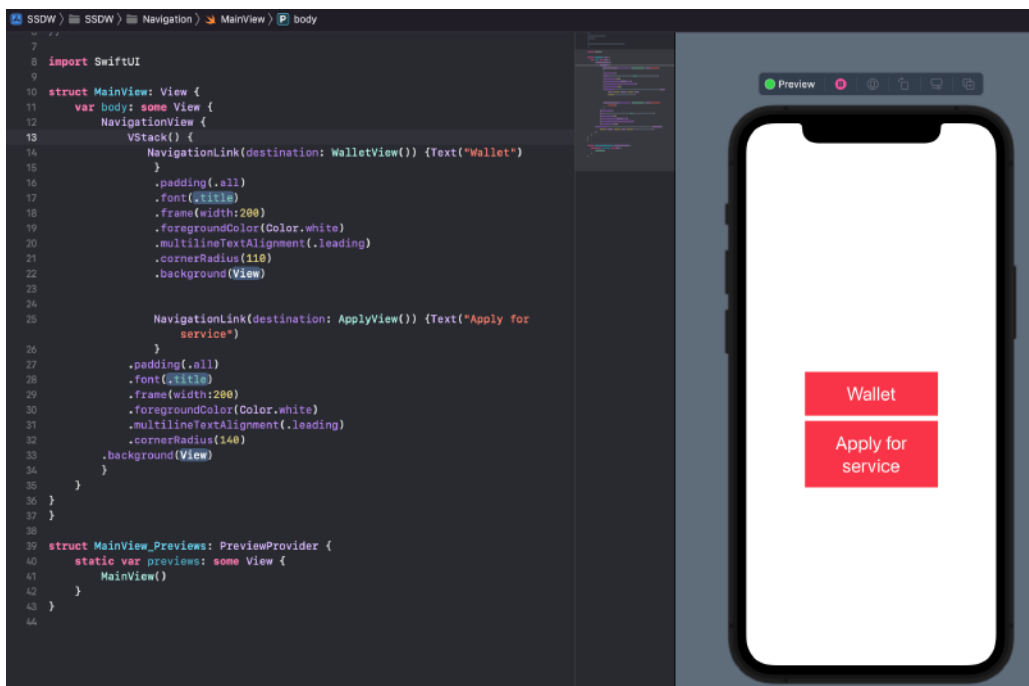


Figure 69: The MainView Screen

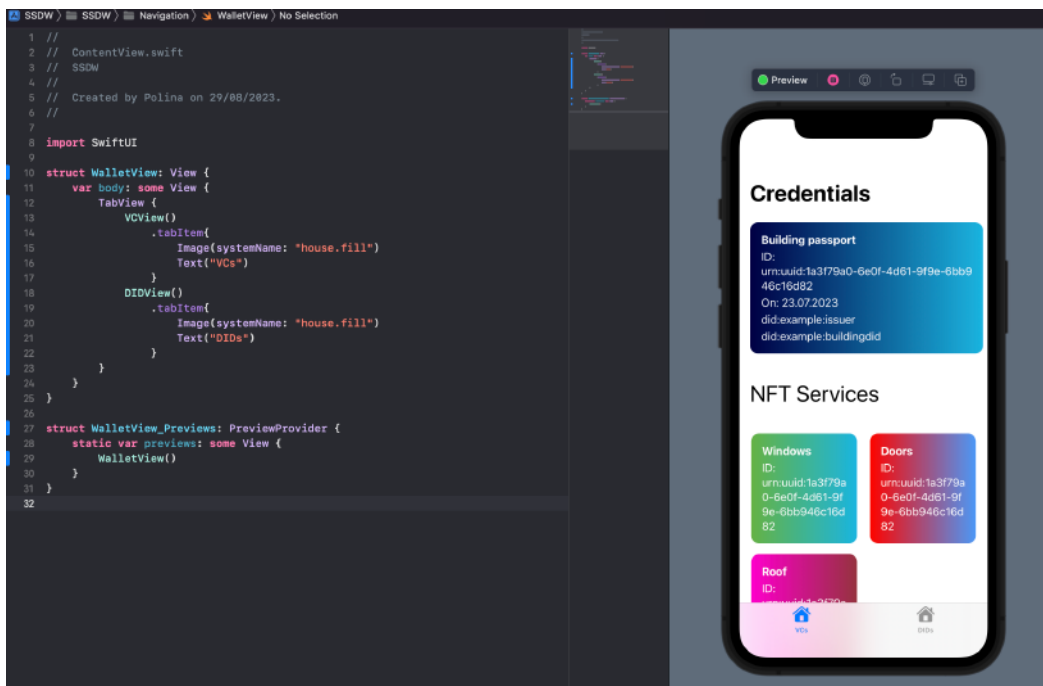


Figure 70: The WalletView VCs Screen

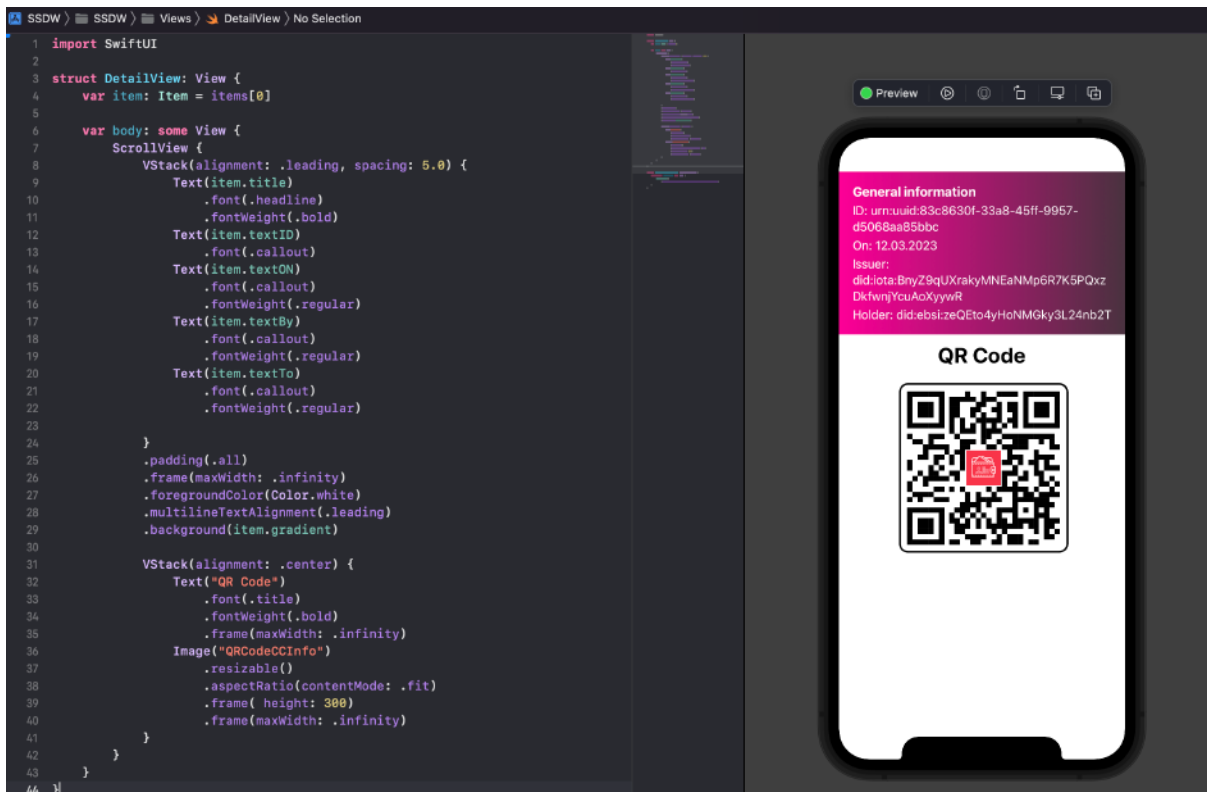


Figure 71: The Detail View of VCs

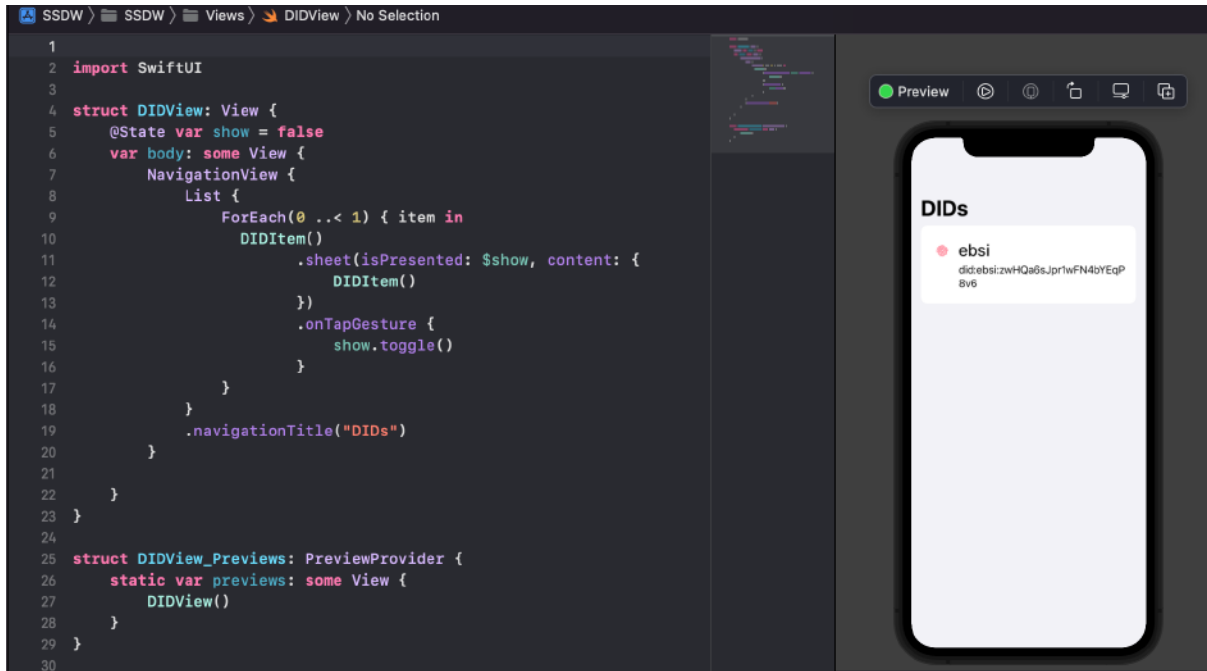


Figure 72: The DIDs Screen

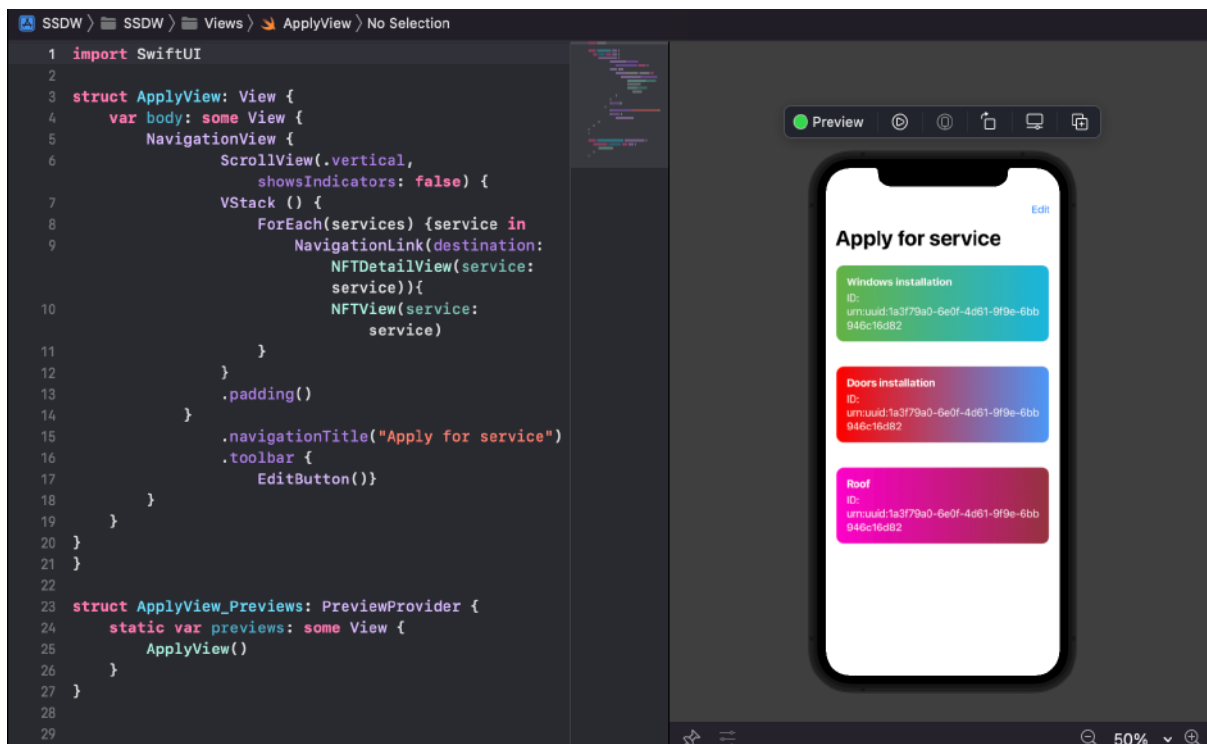


Figure 73: The Apply View Screen

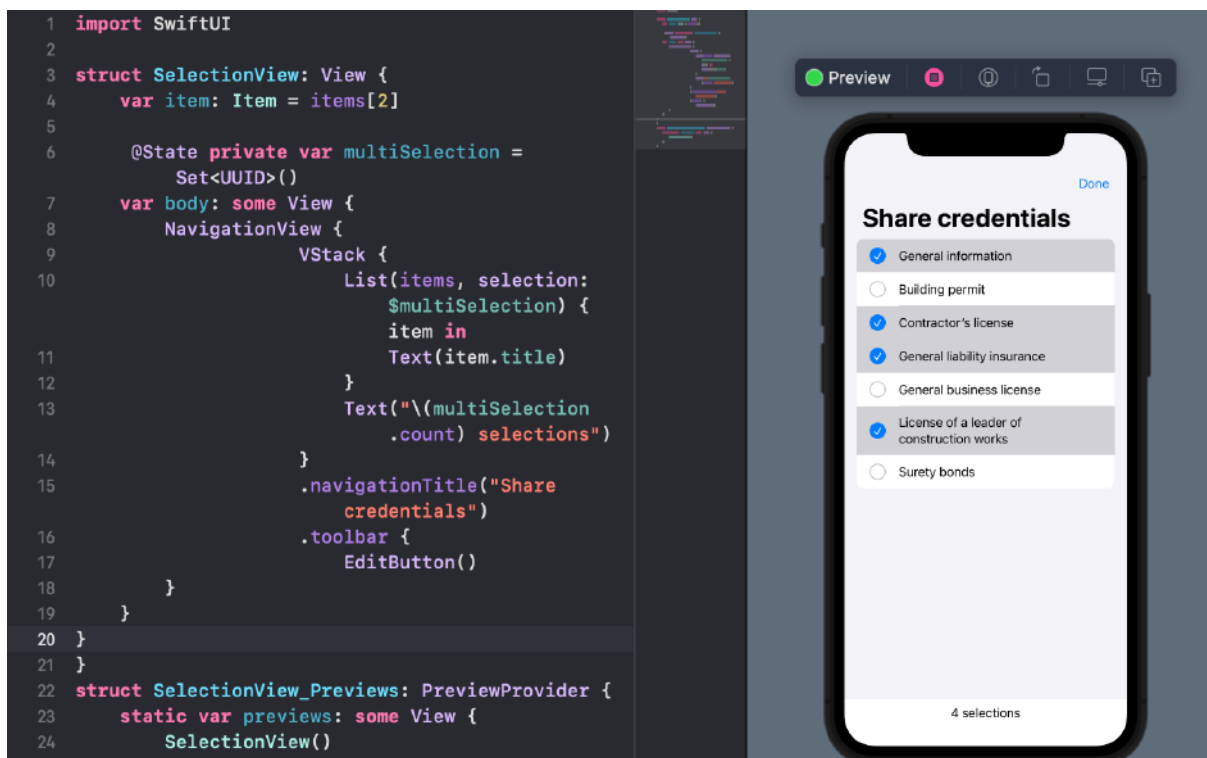


Figure 74: The Share Credentials Screen.

The second option of the SSDW is for the Construction Company. The main view has two directories: SSI wallet and My services.

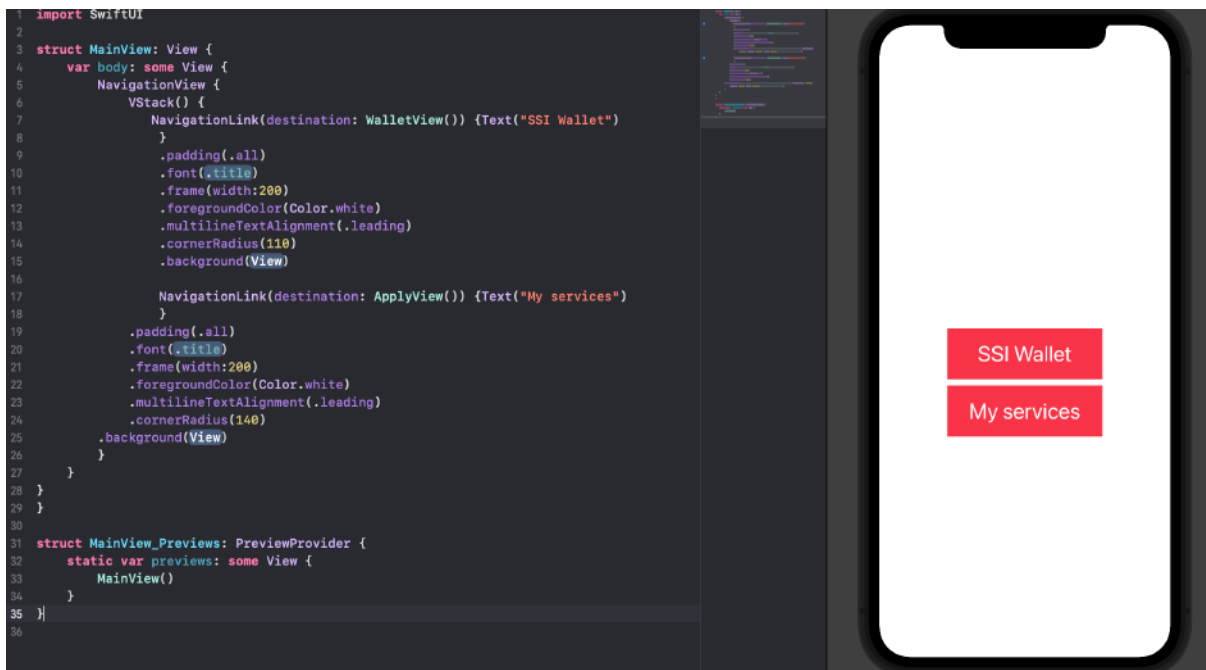


Figure 75: The Construction Company Main View Screen

The SSI Wallet view consists of two sections: "VCs" and "DID." The "VCs" section contains details about issued credentials, NFT services, and IoT data.

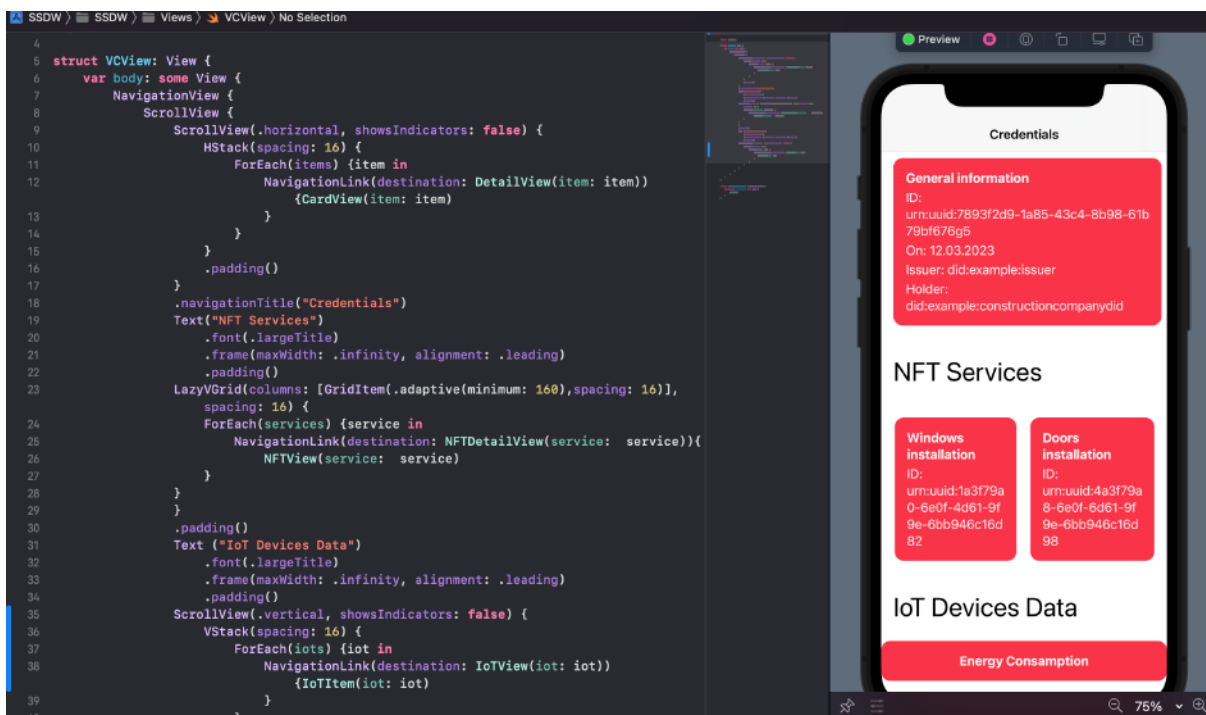


Figure 76: The Construction Company VCs Screen

The "DIDs" section contains details about DIDs.

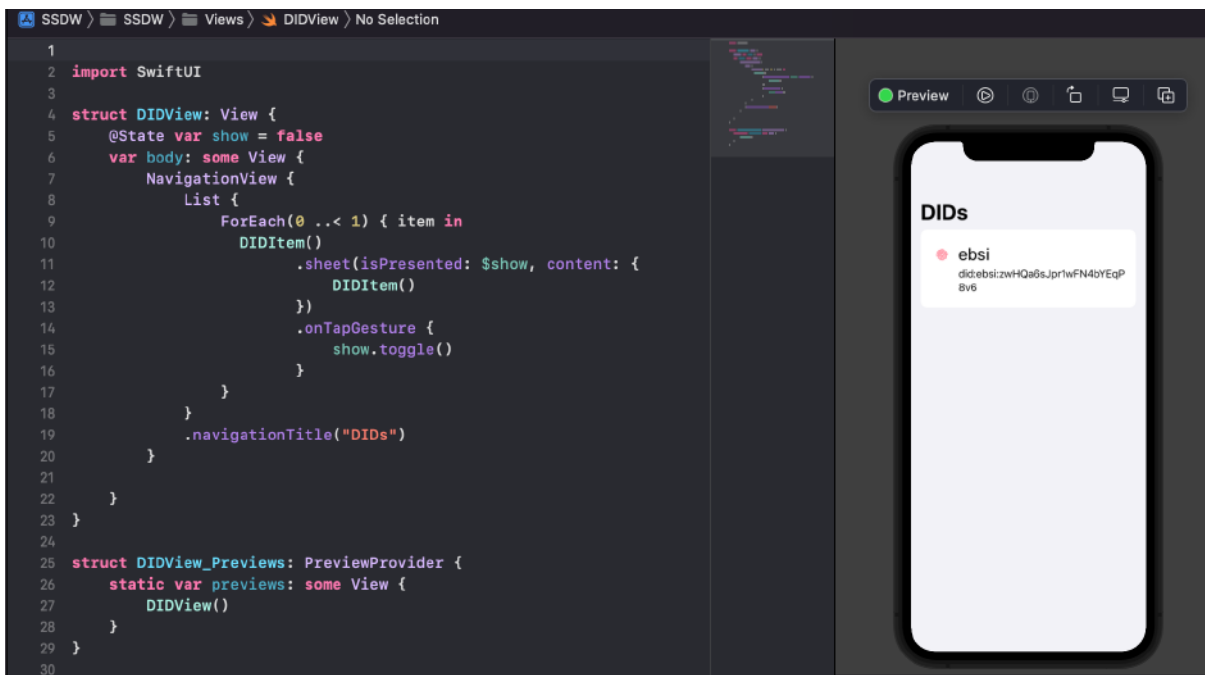


Figure 77: The Construction Company DIDs Screen

The "My Services" section provides information about NFT services obtained from the NFT marketplace.

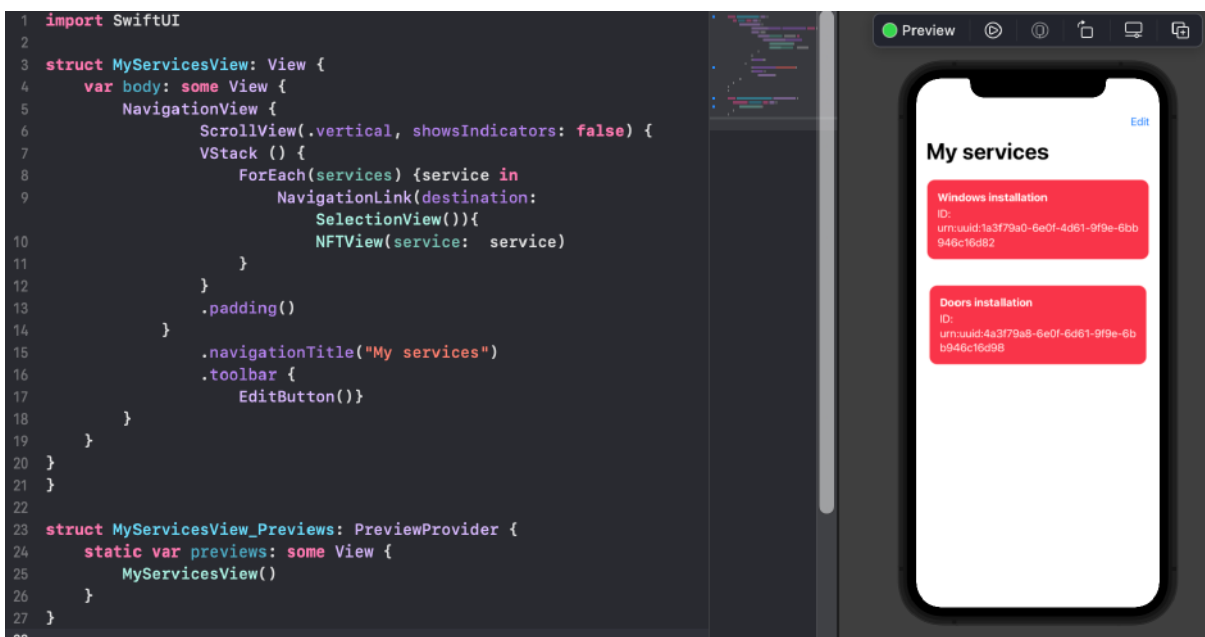


Figure 78: The "My services" screen

The "Share Credentials" screen provides an opportunity to share credentials with other stakeholders.

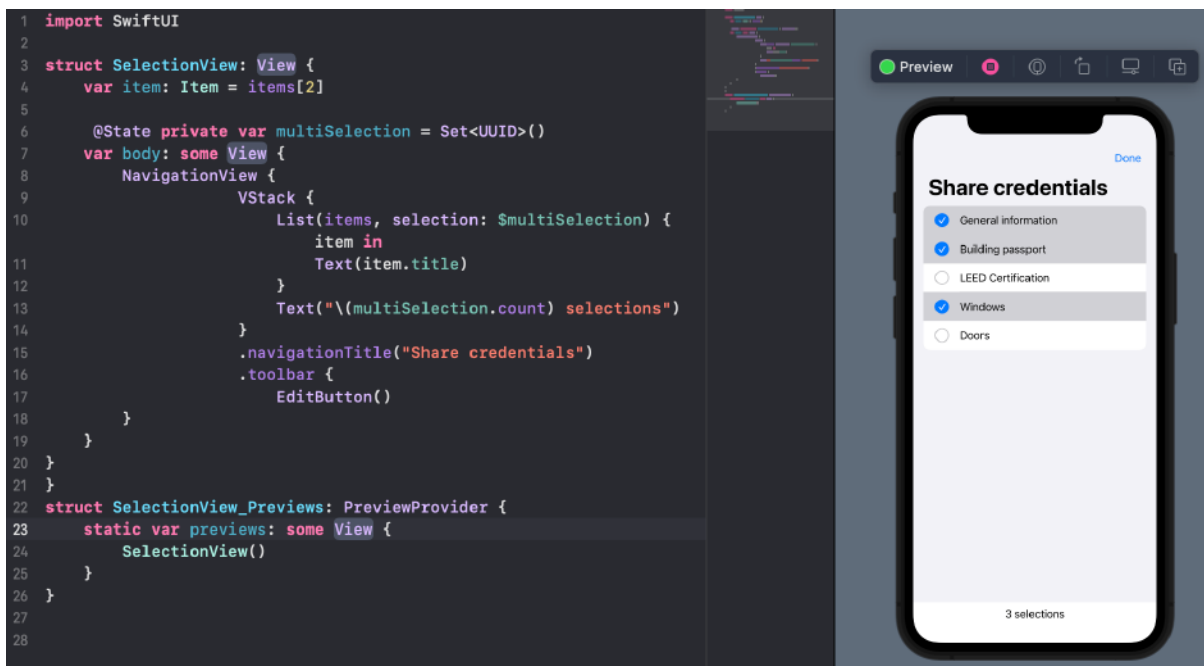


Figure 79: The Share Credentials Screen

The wallet code is available from GitHub repository:

https://github.com/polinasherstobitova/BIMA_SSDW

5 CONCLUSION

The primary objective of this thesis was to construct a secure digital identity management solution and evaluate its applicability within the construction industry using Self-Sovereign Identity. The existing solutions proved to be cumbersome due to lengthy administrative processes and the need for extensive data sharing. To address these challenges, the aim was to create user-friendly, secure, and privacy-respecting identity management solutions, making SSI the most suitable technology.

The outcome of this endeavor is a demo version of a Self-Sovereign Digital Wallet tailored specifically for the construction industry. This achievement was made possible through the utilization of Swift UI and the SSI Kit, resulting in a functional demonstration that highlights the practicality and potential of SSI within this domain. Key components, including templates for VC and DID documents, were meticulously crafted and integrated into the system.

This is a pivotal step towards modernizing the construction industry's identity management processes, emphasizing secure exchanges of data. The incorporation of DIDs serves as a fundamental cornerstone in this proposal. These DIDs, combined with digital wallets, provide unique identification for stakeholders in the construction domain, facilitating secure sharing of project-related VCs through protected digital channels. With SSI and DIDs at the core, contractors and construction companies alike can embrace a new era of trust, connectivity, and innovation within their respective domains. This innovative approach seamlessly aligns with the principles of the IPD process, fostering trust and efficiency.

Our system proposal places a special emphasis on two key roles within the AEC industry: Contractors and Construction Companies. For Contractors, Self-Sovereign Digital Wallets empower them to effectively manage their VCs, encompassing licenses, work permissions, and various qualifications vital to their professional roles. Beyond personal record-keeping, these credentials enable secure applications for construction services while establishing trust and authentication through DIDs.

On the other hand, within Construction Companies, the focus is on managing VCs that encapsulate building-related information. These credentials not only harmonize linked data but can be useful to integrate seamlessly with IoT devices, promoting enhanced data management practices and fostering an interconnected and efficient construction process.

To cater to these diverse needs, the Self-Sovereign Digital Wallet boasts a comprehensive set of features, including the ability to collect VCs, present VP, create DIDs, and manage DID documents. This multifaceted tool, backed by the integration of DIDs, forms the bedrock of our SSI framework, providing stakeholders in the AEC industry with robust control over their digital identities and interactions.

5.1 Future Work

This project opens the door for potential future endeavors in the field of construction industry identity management and SSI. Some possible directions for future work include:

1. **Integration with IoT Devices:** Enhancing the system by seamlessly integrating it with IoT devices. This integration can further improve data management practices and contribute to creating a more interconnected and efficient construction process.
2. **Development of Industry-specific JSON-LD Schemas:** The construction sector can benefit from the development of its own specialized JSON-LD schemas. These schemas can facilitate the structured representation and exchange of construction-related data, contributing to improved interoperability and data standardization within the industry.
3. **Scalability and Real-world Implementation:** Scaling up the digital wallet solution for real-world implementation within the construction industry. This would involve addressing scalability challenges, ensuring compatibility with existing systems, and conducting extensive pilot tests to validate its effectiveness in various construction scenarios.
4. **Privacy and Security Enhancements:** Continuous efforts to enhance the privacy and security aspects of the digital wallet, ensuring that user data remains protected and compliant with evolving data protection regulations.

6 REFERENCES

- Ante, L., Fischer, C. and Strehle, E. (2022) ‘A bibliometric review of research on digital identity: Research streams, influential works and future research paths’, *Journal of Manufacturing Systems*, 62, pp. 523–538. Available at: <https://doi.org/10.1016/J.JMSY.2022.01.005>.
- Bai, Y. *et al.* (2022) ‘Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey’, *Proceedings - 2022 IEEE International Conference on Blockchain, Blockchain 2022*, (2021), pp. 500–507. Available at: <https://doi.org/10.1109/Blockchain55522.2022.00077>.
- Bew, M., & Richards, M. (2008) ‘BIM Maturity Model’, in *Construct IT Autumn 2008 Members’ Meeting*. Brighton, UK.
- Bonduel, M. *et al.* (2018a) ‘The IFC to linked building data converter - Current status’, in *CEUR Workshop Proceedings*.
- Bonduel, M. *et al.* (2018b) ‘The IFC to linked building data converter - Current status’, in *CEUR Workshop Proceedings*. CEUR-WS, pp. 34–43.
- Buldas, A. *et al.* (2022) ‘An Ultra-Scalable Blockchain Platform for Universal Asset Tokenization: Design and Implementation’, *IEEE Access*, 10(July), pp. 77284–77322. Available at: <https://doi.org/10.1109/ACCESS.2022.3192837>.
- CARBONE, A. *et al.* (2018) ‘Blockchain based Distributed Cloud Fog Platform for IoT Supply Chain Management’, in. Available at: <https://doi.org/10.15224/978-1-63248-144-3-37>.
- Chen, Y. *et al.* (2022) ‘Construction 4.0, Industry 4.0, and Building Information Modeling (BIM) for Sustainable Building Development within the Smart City’, *Sustainability (Switzerland)*, 14(16). Available at: <https://doi.org/10.3390/su141610028>.
- Clauß, S. and Köhntopp, M. (2001) ‘Identity management and its support of multilateral security’, *Computer Networks*, 37(2), pp. 205–219. Available at: [https://doi.org/10.1016/S1389-1286\(01\)00217-1](https://doi.org/10.1016/S1389-1286(01)00217-1).
- Cocco, L., Tonelli, R. and Marchesi, M. (2022) ‘A System Proposal for Information Management in Building Sector Based on BIM , SSI , IoT and Blockchain’.

Dhamija, R. and Dusseault, L. (2008) ‘The seven flaws of identity management: Usability and security challenges’, *IEEE Security and Privacy*, 6(2). Available at: <https://doi.org/10.1109/MSP.2008.49>.

Fedrecheski, G. *et al.* (2020) ‘Self-Sovereign Identity for IoT environments: A Perspective’, in *GIoTS 2020 - Global Internet of Things Summit, Proceedings*. Available at: <https://doi.org/10.1109/GIOTS49054.2020.9119664>.

Gill, S.S. *et al.* (2019) ‘Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges’, *Internet of Things (Netherlands)*. Available at: <https://doi.org/10.1016/j.iot.2019.100118>.

Goh, C.S., Su, F. and Rowlinson, S. (2023) ‘Exploring Economic Impacts of Sustainable Construction Projects on Stakeholders: The Role of Integrated Project Delivery’, *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 15(3). Available at: <https://doi.org/10.1061/jladah.ladr-963>.

Goode, A. (2019) ‘Digital identity: solving the problem of trust’, *Biometric Technology Today*, 2019(10), pp. 5–8. Available at: [https://doi.org/10.1016/S0969-4765\(19\)30142-0](https://doi.org/10.1016/S0969-4765(19)30142-0).

Hiremath, B.K. and Kenchakkanavar, A.Y. (2016) ‘An Alteration of the Web 1.0, Web 2.0 and Web 3.0: A Comparative Study’, *Imperial Journal of Interdisciplinary Research*, 2(4), pp. 2454–1362. Available at: <http://www.imperialjournals.com/index.php/IJIR/article/view/327/320>.

Hofmann, E. and Rüsç, M. (2017) ‘Industry 4.0 and the current status as well as future prospects on logistics’, *Computers in Industry*, 89, pp. 23–34. Available at: <https://doi.org/10.1016/J.COMPIND.2017.04.002>.

Janowicz, K. *et al.* (2020) ‘BOT: The building topology ontology of the W3C linked building data group’, in *Semantic Web*. Available at: <https://doi.org/10.3233/SW-200385>.

Jung, N. and Lee, G. (2019) ‘Automated classification of building information modeling (BIM) case studies by BIM use based on natural language processing (NLP) and unsupervised learning’, *Advanced Engineering Informatics*, 41, p. 100917. Available at: <https://doi.org/10.1016/J.AEI.2019.04.007>.

Kochovski, P. *et al.* (2019) ‘Trust management in a blockchain based fog computing platform with trustless smart oracles’, *Future Generation Computer Systems*, 101. Available at: <https://doi.org/10.1016/j.future.2019.07.030>.

Kochovski, P. and Stankovski, V. (2018) ‘Supporting smart construction with dependable edge computing infrastructures and applications’, *Automation in Construction*, 85. Available at: <https://doi.org/10.1016/j.autcon.2017.10.008>.

Kochovski, P. and Stankovski, V. (2020) ‘Algorithms for a Smart Construction Environment’, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Available at: https://doi.org/10.1007/978-3-030-58628-7_1.

Kochovski, P. and Stankovski, V. (2021) ‘Building applications for smart and safe construction with the DECENTER Fog Computing and Brokerage Platform’, *Automation in Construction*, 124. Available at: <https://doi.org/10.1016/j.autcon.2021.103562>.

König, M. *et al.* (2011) ‘Information modelling for sustainable buildings’, in *ACM International Conference Proceeding Series*. Available at: <https://doi.org/10.1145/2095536.2095641>.

Krijnen, T. and Beetz, J. (2018) ‘A SPARQL query engine for binary-formatted IFC building models’, *Automation in Construction*, 95, pp. 46–63. Available at: <https://doi.org/10.1016/j.autcon.2018.07.014>.

Maniatis, D.A. (2022) *Industrial Internet of Things Attack Vectors, Challenges, and Mitigations for the Realization of Industry 4.0. Case Study : A Proposed Framework for Cybersecurity in Iot Using SSI in Wind Turbines*. Available at: https://doi.org/10.26267/unipi_dione/2359.

Nagaroor, R. (2008) ‘Analysis and Evaluation of Blockchain-based Self-Sovereign Identity Systems’, *Conference on Algebra and ...* [Preprint].

Oraskari, J. and Törmä, S. (2015a) ‘RDF-based signature algorithms for computing differences of IFC models’, *Automation in Construction*, 57, pp. 213–221. Available at: <https://doi.org/10.1016/J.AUTCON.2015.05.008>.

Oraskari, J. and Törmä, S. (2015b) ‘RDF-based signature algorithms for computing differences of IFC models’, *Automation in Construction*, 57, pp. 213–221. Available at: <https://doi.org/10.1016/j.autcon.2015.05.008>.

Pan, Y. and Zhang, L. (2023) ‘Integrating BIM and AI for Smart Construction Management: Current Status and Future Directions’, *Archives of Computational Methods in Engineering*, 30(2), pp. 1081–1110. Available at: <https://doi.org/10.1007/s11831-022-09830-8>.

Pärn, E.A., Edwards, D.J. and Sing, M.C.P. (2017) ‘The building information modelling trajectory in facilities management: A review’, *Automation in Construction*, 75, pp. 45–55. Available at: <https://doi.org/10.1016/J.AUTCON.2016.12.003>.

Pauwels, P. *et al.* (2023) ‘Live semantic data from building digital twins for robot navigation: Overview of data transfer methods’, *Advanced Engineering Informatics*, 56, p. 101959. Available at: <https://doi.org/10.1016/J.AEI.2023.101959>.

Pauwels, P. *et al.* (2012) ‘Discussion and Workshop Conclusions: Supporting Decision-Making in the Building Lifecycle using Linked Data’, in.

Preukschat, Alex, and D.R. (2021) *Self-sovereign identity*. Manning Publications.

Reed, D., Allen, C. and Vogelsteller, F. (no date) *Self-Sovereign Identity*.

Reed, D., Sporny, M. and Allen, C. (2019) ‘Decentralized Identifiers (DIDs) v1.0’, *W3C* [Preprint], (November).

Satybaldy, A. (2023) ‘Usability Evaluation of SSI Digital Wallets BT - Privacy and Identity Management’, in F. Bieker *et al.* (eds). Cham: Springer Nature Switzerland, pp. 101–117.

Sawhney, A. *et al.* (2020) ‘A proposed framework for Construction 4.0 based on a review of literature’, 1, pp. 301–291. Available at: <https://doi.org/10.29007/4nk3>.

Serrano, W. (2023) ‘Smart or Intelligent Assets or Infrastructure: Technology with a Purpose’, *Buildings*, 13(1). Available at: <https://doi.org/10.3390/buildings13010131>.

Simmonds, P. (2015) ‘The digital identity issue’, *Network Security*, 2015(8), pp. 8–13. Available at: [https://doi.org/10.1016/S1353-4858\(15\)30069-6](https://doi.org/10.1016/S1353-4858(15)30069-6).

Taherizadeh, S., Stankovski, V. and Grobelnik, M. (2018) 'A capillary computing architecture for dynamic internet of things: Orchestration of microservices from edge devices to fog and cloud providers', *Sensors (Switzerland)*, 18(9). Available at: <https://doi.org/10.3390/s18092938>.

Tang, S. and Shelden, D.R. (2020) 'A Framework Utilizing Modern Data Models with IFC for Building Automation System Applications', in *Construction Research Congress 2020: Computer Applications - Selected Papers from the Construction Research Congress 2020*. American Society of Civil Engineers (ASCE), pp. 11–19. Available at: <https://doi.org/10.1061/9780784482865.002>.

Teisserenc, B. and Sepasgozar, S.M.E. (2022) 'Software Architecture and Non-Fungible Tokens for Digital Twin Decentralized Applications in the Built Environment', *Buildings*, 12(9). Available at: <https://doi.org/10.3390/buildings12091447>.

Tobin, A. and Reed, D. (2017) 'The Inevitable Rise of Self-Sovereign Identity', *White paper*, 29(September 2016).

Torino, P.D.I. (2022) *Self-Sovereign-Identity as a Service*.

Vasiliu-Feltes, Ingrid, Mysore, I. (2022) *Digital Identity in the New Era of Personalized Medicine*.

Verifiable Credentials Data Model v1.1 W3C Recommendation 03 March 2022 (no date). Available at: <https://www.w3.org/TR/vc-data-model/>.

Wang, T., Zhang, S. and Liew, S.C. (2023) 'Linking Souls to Humans with ZKBID: Accountable Anonymous Blockchain Accounts for Web 3.0 Decentralized Identity', pp. 1–16. Available at: <http://arxiv.org/abs/2301.02102>.

Wong, J.K.W. and Zhou, J. (2015) 'Enhancing environmental sustainability over building life cycles through green BIM: A review', *Automation in Construction*, 57, pp. 156–165. Available at: <https://doi.org/10.1016/J.AUTCON.2015.06.003>.

Y. Jing, J. Li, Y.W. and H.L. (2021) 'The Introduction of Digital Identity Evolution and the Industry of Decentralized Identity', in *3rd International Academic Exchange Conference on*

Science and Technology Innovation (IAECST). Guangzhou, China: IEEE, pp. 504–508.
Available at: <https://doi.org/10.1109/IAECST54258.2021.9695553>.

Zhu, J., Wu, P. and Lei, X. (2023) ‘IFC-graph for facilitating building information access and query’, *Automation in Construction*, 148. Available at: <https://doi.org/10.1016/j.autcon.2023.104778>.