Technische Hochschule
Brandenburg
University of
Applied Sciences

Self-sovereign Identity: Development of an Implementation-based Evaluation Framework for Verifiable Credential SDKs

Brandenburg University of Applied Sciences
Department of Economics

Master's Thesis

submitted by
Philipp Bolte
July 14, 2021

First supervisor: Prof. Dr. rer. nat. Vera G. Meister
Second supervisor: Jonas Jetschni, M.Sc.

Statutory Declaration

I hereby attest that I have written this thesis independently without any outside help and that I have used only the sources cited.

Brandenburg, July 14, 2021

Philipp Bolte

Abstract

Diese LaTeX-Vorlage ist für Berichte, Bachelor- sowie Masterarbeiten gedacht. Natürlich ist sie nicht perfekt und jede Art der Verbesserung wird dankend angenommen. Bei Fragen zur Verwendung oder Anregungen zur Verbesserung können Sie mir diese gern an markus.brandt1992@gmail.com senden.

An entsprechender Stelle werden Beispiele für die Verwendung von Abkürzungen, Zitaten, Abbildungen, Tabellen und die Einbettung von Code gegeben.

Contents

List of Figures

List of Tables

List of Abbreviations

DID Decentralized Identifier

SSI Self-sovereign Identity

VC Verifiable Credential

VP Verifiable Presentation

1 Introduction

The Internet has become a cornerstone of coexistence in today's world. With over 4.66 billion Internet users worldwide [Jo21], it determines how we communicate, think, inform ourselves, and interact with one another. As a result, huge networks of people are being created in which different cultures are coming closer together and knowledge is being shared like never before. A central enabler for the functioning of such interactions are digital identities, which are gaining an increasingly important role [Li20].

Over the course of our lives, we collect a large amount of digital identities from a wide variety of services, including Facebook, Twitter, WhatsApp, GitHub, LinkedIn, and many more. Because of the way we manage digital identities in the current era, users mostly own separate identities for each service or go through centralized, federated identity providers like Google or Facebook. As a result of these key developments, silos of identity data emerged, which are problematic concerning efficiency, security, and privacy. Several historical data leaks and hacks in which sensitive user data was made public show that these approaches are not suitable for managing sensitive user data. [Sw21]. [Eh21]

In contrast, the Self-sovereign Identity (SSI) paradigm takes a new approach by giving back users control of their digital identities through various novel approaches. This thesis explores this new approach from a developer's point of view. In the next sections, the objectives, related work and the research approach will be discussed.

1.1 Objectives

For a successful realization of Self-sovereign Identity (SSI) concepts, the existence of good solutions for developers is critical. This ensures that the barriers to a successful adoption of SSI are kept to a minimum, simplifying and speeding up the entire process. A good toolset and developer experience is thus a key enabler for SSI.

With this in mind, an overview of the most important solutions[1] in the SSI space will be established throughout the thesis. To scope the work accordingly, this thesis looks at the solutions in terms of how closely they can map the lifecycle of a Verifiable Credential (VC). It is intended to serve as an entry point for developers to get an overview of the capabilities of existing solutions and to give starting points for further research. Furthermore, a use case agnostic reference implementation is presented that implements four of the presented solutions based on the lifecycle. It can serve developers as a basis for their own work, but above all enables practical validation and the gathering of experience during its development. In this way, the knowledge gained flows directly into a new evaluation framework, which, in addition to other software selection frameworks, can provide concrete

[1] synonymous to SDKs, libraries, frameworks, and platforms

help in selecting the most suitable solution from the developer's point of view. In addition, it can reveal shortcomings in current solutions that need to be addressed for successful adoption of SSI in practical use cases. So the objective of this work, besides the scientific contributions, is to generate added value for the whole ecosystem.

1.2 Related Work

At the current time, there does not appear to be any comparable work that addresses the topic in a manner corresponding to Section 1.1. The most similar is [NJ20] who have developed a mobile wallet based on uPort that covers login, VC issuance as well as verification. Based on the experience gained, an evaluation of uPort has been made as well.However, uPort is currently no longer being developed, and the assessment is also based on only a fraction of the VC lifecycle and basic principles for SSI.

Another paper by [Ku20] defines a comprehensive evaluation framework from an enterprise perspective that, compared to other papers, also covers aspects such as user experience, technology and compliance. It is characterized by a wide range of questions that are used for the evaluation of 43 solutions. However, the list of solutions considered is outdated and missing important players (see e.g. MATTR and Trinsic). Furthermore, the assessment does not provide any practical guidance for developers. A clear analysis of the SSI-relevant features, e.g. with regard to the VC lifecycle, does not exist.

Otherwise, many papers seem to focus on theoretical foundations or evaluation of existing solution based on two things: (i) architecture [GMM18] concerning privacy [Be19], performance [Bo20], use case [Ku20], various variations [Al16, Re21, AL20, Bo20, FCA19, Ca05] of SSI principles [Bo19, Bo20, DT20, DP18, FCA19, SNE20], and (ii) the interoperability between those systems [Ho20, Jo20]. This clearly shows that there is a deficit in terms of works that look at existing solutions based on their practical features and applicability from a developer's point of view. This thesis addresses some of these gaps and thus clearly contributes to the field of research.

1.3 Methodology

2 Grundlagen

2.1 Abkürzungen

Abkürzungen im Text lassen ....

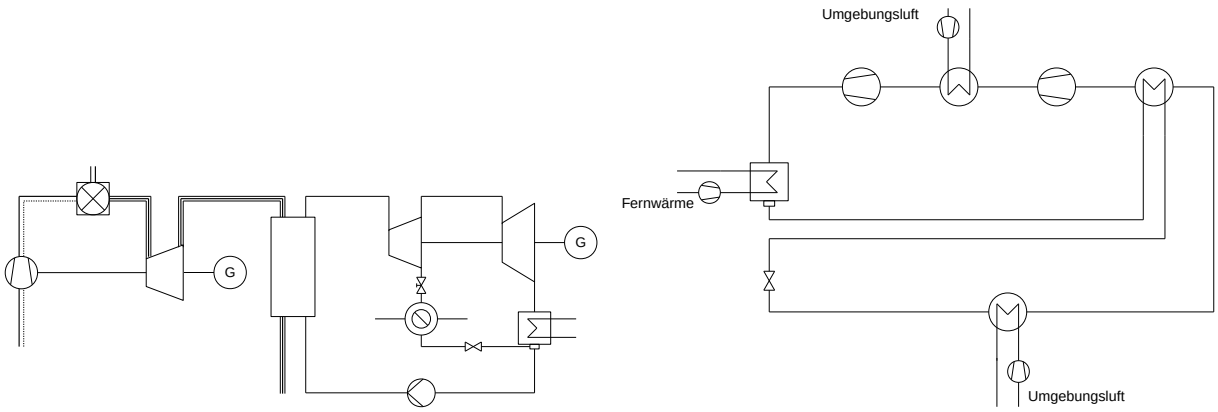
2.2 Quellenangaben

Nach ... kann angenommen werden, dass ...

Energie besteht aus Exergie und Anergie.

2.3 Abbildungen

In Abbildung 2.1 ist zu erkennen, dass ...



(a) Gas- und Dampfkraftwerk **(b)** Wärmepumpe

Figure 2.1: Abbildung 2.1a zeigt das Wärmeschaltbild eines Gas- und Dampfkraftwerks mit einer einfachen Entnahme im Dampfturbinen Teil. Abbildung 2.1b zeigt hingegen das Schaltbild einer Kompressionswärmepumpe mit einfacher Kondensatunterkühlung.

2.4 Tabellen

Durch das Hinzufügen von Fußnoten innerhalb einer Tabelle können zusätzliche Informationen zu bestimmten Werten oder Bezeichnungen gegeben werden. In Tabelle 2.1 gibt die Fußnote an, dass die angegebene Grädigkeit für alle Wärmeübertrager gleichermaßen gilt.

Table 2.1: Auslegungsparameter des Gas- und Dampfkraftwerks

Teilprozess	Parameter	Symbol	Einheit	Wert
Fernwärme	Vorlauftemperatur	T_{VL}	°C	124
	Rücklauftemperatur	T_{RL}	°C	50
	Druck	p_{FW}	bar	10
	Wärmeaufnahme	$\dot{Q}_{\mathrm{DH}}$	MW	145
Gasturbinenprozess	Brennstoffmassenstrom	$\dot{m}_{\mathrm{Fuel}}$	kg/s	11,58
	Umgebungstemperatur	T_{U}	°C	20
	Verbrennunstemperatur	T_{CC}	°C	1500
	Abgastemperatur	T_{AG}	°C	150
	Verdichterdruckverhältnis	pr	-	14
	Verdichterwirkungsgrad	η_{V}	-	0,91
	Gasturbinenwirkungsgrad	η_{GT}	-	0,9
Dampfturbinenprozess	Frischdampftemperatur	T_{FD}	°C	600
	Frischdampfdruck	p_{FD}	bar	100
	Entnahmedruck	p_{E}	bar	3
	Abdampfdruck	p_{AD}	bar	0,04
	Dampfturbinenwirkungsgrad	η_{DT}	-	0,9
	Pumpenwirkungsgrad	η_{P}	-	0,8
	Grädigkeit[1]	ΔT	K	5

[1] Grädigkeit wird für alle verwendeten Wärmeübertrager gleich angenommen.

2.5 Code

Die Darstellung von Code erfolgt über das Paket *listings*. Einstellung dazu sind in der Präambel zu finden. Ein Beispiel für Code in LaTeX:

```
import numpy as np

def pi(n):
    t = 0
    for i in range(n):
        x = np.random.rand()
        y = np.random.rand()

        if np.sqrt(x**2 + y**2) <= 1:
            t += 1
    return 4 * (t / n)
```

3 Hauptteil

3.1 Abschnitt 1

3.2 Abschnitt 2

3.3 Abschnitt 3

4 Ergebnisse

4.1 Abschnitt 1

4.2 Abschnitt 2

4.3 Abschnitt 3

5 Diskussion der Ergebnisse

5.1 Schlussfolgerungen

5.2 Kritische Betrachtung

5.3 Ausblick

Bibliography

[Al16] Allen, Christopher: , The Path to Self-Sovereign Identity, April 2016.

[AL20] Allende López, Marcos: Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain. Inter-American Development Bank, September 2020.

[Be19] Bernabe, J. Bernal; Canovas, J. L.; Hernandez-Ramos, J. L.; Moreno, R. Torres; Skarmeta, A.: Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access, 7:164908–164940, 2019. Conference Name: IEEE Access.

[Bo19] van Bokkem, Dirk; Hageman, Rico; Koning, Gijs; Nguyen, Luat; Zarin, Naqib: Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. arXiv:1904.12816 [cs], April 2019. arXiv: 1904.12816.

[Bo20] Bouras, Mohammed Amine; Lu, Qinghua; Zhang, Fan; Wan, Yueliang; Zhang, Tao; Ning, Huansheng: Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2):483, January 2020.

[Ca05] Cameron, Kim: , The Laws of Identity, May 2005.

[DP18] Dunphy, Paul; Petitcolas, Fabien A.P.: A First Look at Identity Management Schemes on the Blockchain. IEEE Security & Privacy, 16(4):20–29, July 2018.

[DT20] Dib, Omar; Toumi, Khalifa: Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. Annals of Emerging Technologies in Computing, 4(5):19–40, December 2020.

[Eh21] Ehrlich, Tobias; Richter, Daniel; Meisel, Michael; Anke, Jürgen: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD Praxis der Wirtschaftsinformatik, February 2021.

[FCA19] Ferdous, Md Sadek; Chowdhury, Farida; Alassafi, Madini O.: In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access, 7:103059–103079, 2019.

[GMM18] Grüner, Andreas; Mühle, Alexander; Meinel, Christoph: On the Relevance of Blockchain in Identity Management. arXiv:1807.08136 [cs], July 2018. arXiv: 1807.08136.

[Ho20] Homeland Security: , Preventing Forgery & Counterfeiting of Certificates and Licenses – Phase 1 Interoperability Plug Fest Test Plan, May 2020.

[Jo20] John, Anil: , DHS SVIP Blockchain/DLT/SSI Cohort - Multi-Product Phase 1 Interop Artifacts/ Scaffolding / Information, December 2020.

[Jo21] Johnson, Joseph: , Internet users in the world 2021, July 2021.

[Ku20] Kuperberg, Michael: Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. IEEE Transactions on Engineering Management, 67(4):1008–1027, November 2020.

[Li20] Liu, Yang; He, Debiao; Obaidat, Mohammad S.; Kumar, Neeraj; Khan, Muhammad Khurram; Raymond Choo, Kim-Kwang: Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, 166, September 2020.

[NJ20] Naik, Nitin; Jenkins, Paul: uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain. In: 2020 IEEE International Symposium on Systems Engineering (ISSE). IEEE, Vienna, Austria, pp. 1–7, October 2020.

[Re21] Reed, Drummond; Sporny, Manu; Longley, Dave; Allen, Christopher; Grant, Ryan; Sabadello, Markus: , Decentralized Identifiers (DIDs) v1.0, March 2021.

[SNE20] Satybaldy, Abylay; Nowostawski, Mariusz; Ellingsen, Jørgen: Self-Sovereign Identity Systems: Evaluation Framework. In (Friedewald, Michael; Önen, Melek; Lievens, Eva; Krenn, Stephan; Fricker, Samuel, eds): Privacy and Identity Management. Data for Better Living: AI and Privacy, volume 576, pp. 447–461. Springer International Publishing, Cham, 2020. Series Title: IFIP Advances in Information and Communication Technology.

[Sw21] Swinhoe, Dan: , The 15 biggest data breaches of the 21st century, January 2021.

A Appendix