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 13, 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 13, 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

1 Introduction **1**
- 1.1 Motivation . . . 1
- 1.2 Related Work . . . 2
- 1.3 Methodology . . . 2

2 Grundlagen **3**
- 2.1 Abkürzungen . . . 3
- 2.2 Quellenangaben . . . 3
- 2.3 Abbildungen . . . 3
- 2.4 Tabellen . . . 4
- 2.5 Code . . . 4

3 Hauptteil **5**
- 3.1 Abschnitt 1 . . . 5
- 3.2 Abschnitt 2 . . . 5
- 3.3 Abschnitt 3 . . . 5

4 Ergebnisse **7**
- 4.1 Abschnitt 1 . . . 7
- 4.2 Abschnitt 2 . . . 7
- 4.3 Abschnitt 3 . . . 7

5 Diskussion der Ergebnisse **9**
- 5.1 Schlussfolgerungen . . . 9
- 5.2 Kritische Betrachtung . . . 9
- 5.3 Ausblick . . . 9

Literaturverzeichnis **10**

A Appendix **13**

List of Figures

2.1 Gegenüberstellung Gas- und Dampfkraftwerk mit Wärmepumpe 3

List of Tables

2.1 Auslegungsparameter des Gas- und Dampfkraftwerks 4

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 [1], 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 in our lives [2].

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, ORCID, 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, centralized silos of identity data emerged, which are problematic concerning efficiency, security, and privacy. That this is problematic is shown by various historical data leaks and hacks in which sensitive user data was made public [3]. [4]

In contrast, the Self-sovereign Identity (SSI) paradigm takes a new approach in trying to give users back control of their digital identities through various novel approaches. This paradigm is picked up by this work and looked at from the point of view of a developer. In the next sections, the objectives, related work and the research approach will be discussed.

1.1 Motivation

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 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 implementation. In this way, the knowledge gained flows directly into a new evaluation framework, which, in addition to other software selection frameworks, can provide very

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

concrete help in selecting the most suitable solution from the developer's point of view. Thus, this thesis introduces three new practical tools that may help in the adoption of SSI by empowering developers.

1.2 Related Work

1.3 Methodology

2 Grundlagen

2.1 Abkürzungen

Abkürzungen im Text lassen sich mit dem Paket *acronym* verwenden:
4GDH! (**4GDH!**)
Bei der nächsten Verwendung im Text wird dann nur noch die Abkürzung verwendet **4GDH!**

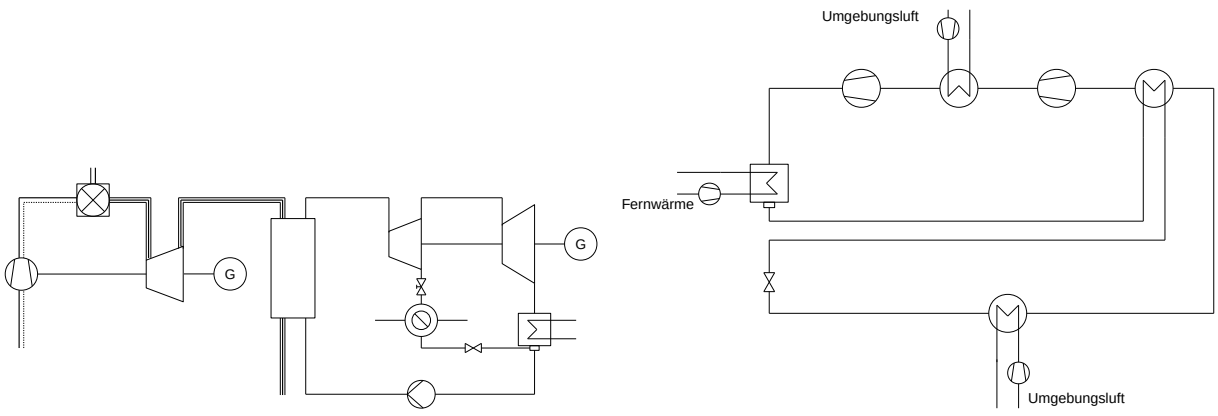
2.2 Quellenangaben

Nach [5] kann angenommen werden, dass ...

Energie besteht aus Exergie und Anergie [6, S. 15].

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

[1] J. Johnson, "Internet users in the world 2021," July 2021.

[2] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, Sept. 2020.

[3] D. Swinhoe, "The 15 biggest data breaches of the 21st century," Jan. 2021.

[4] T. Ehrlich, D. Richter, M. Meisel, and J. Anke, "Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten," *HMD Praxis der Wirtschaftsinformatik*, Feb. 2021.

[5] European Commission. Joint Research Centre., *Blockchain in education.* LU: Publications Office, 2017.

[6] T. Weingärtner and O. Camenzind, "Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices," vol. 4, no. 1, 2021.

A Appendix