Frankfurt University of Applied Sciences

–Faculty of Computer Science and Engineering–

The Design and Evaluation of a Wallet-based IoT Identity Management Framework for Smart Vehicles

Abschlussarbeit zur Erlangung des akademischen Grades

Master of Science (M.Sc.)

vorgelegt von

Hendrik Pfaff

Matrikelnummer: 1319114

Referent	:	Prof Dr. Nils Urbach
Korreferent	:	Simon Feulner, M.Sc.

EIDESSTATTLICHE ERKLÄRUNG

Ich versichere hiermit, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Frankfurt, 31. August 2023

Hendrik Pfaff

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to all those who have supported me throughout the work completing this Master's Thesis and my studies. The completion of this work would not have been possible without the collective effort and encouragement of all these remarkable individuals.

First and foremost, I extend my heartfelt thanks to my loving girlfriend, Helen, whose never ending support, patience, understanding and professional advice - not only during the challenging phases of this thesis - have been a reliable backing to me. I am also grateful to my thesis advisors, Simon Feulner and Vincent Gramlich, for their expert guidance, insightful feedback, and continuous encouragement as well as Dr. Nils Urbach for allowing me to work on this topic under his supervision. Thanks to your patience, time and effort, I was able to write this thesis the way I did. I would also like to acknowledge my superiors and my colleagues at *esatus AG*, whose understanding and professional expertise made it possible for me to enter the topic of decentralized identity in the first place. Not only did the positive work environment you created, enabled me to work on this thesis and at work at the same time, but also did our valuable discussions of numerous ideas proofed to be crucial to my understanding of various topics.

My heartfelt appreciation also goes out to the experts who graciously agreed to be interviewed for this project and spend hours of their time answering my questions. Your insights and expertise during the evaluation of my framework have enriched the content of this thesis, lending perspectives that otherwise would have been unattainable to me.

Each of you has played an integral role in shaping my academic work and I am truly grateful for this opportunity.

ABSTRACT

The increasing integration of Internet of Things (IoT) devices into urban environments and our every day "smart" vehicles mark a significant transformation in the way our cities and vehicles operate and interact with each other. While the establishment of new low emission zones, congestion charge areas or other restrictive city policies become the reason for ever more sophisticated traffic monitoring and identification systems, the limitations of those technical solutions become apparent. In this master's thesis, I introduce a wallet-based identity management framework for smart vehicles, to tackle some of the challenges of the traditional approaches of vehicle identification in modern urban cities. By presenting the frameworks architecture containing all participating entities as well as the processes necessary to fulfill its goal of vehicle and driver identification, I point out an alternative approach in terms of vehicular monitoring in smart city scenarios. To ensure scientific rigor in this thesis, I apply the iterative Design Science Research (DSR) methodology, in which the framework is designed with its requirements and design objectives in mind, evaluated by conducting expert interviews, and then revised to incorporate the newly found insights. In conclusion, I demonstrate the key findings of the elaborate evaluation process, the benefits of using this framework for real world vehicle identification, and the remaining challenges to build upon in future research.

ABSTRAKT

Die zunehmende Integration von IoT-Geräten in städtische Umgebungen und unsere alltäglichen smarten Fahrzeugen bedeutet einen immensen Wandel in der Art und Weise, wie unsere Städte und Fahrzeuge funktionieren und miteinander interagieren. Während die Einrichtung neuer Umweltzonen, Mautgebiete oder anderer restriktiver städtischer Maßnahmen zum Anlass für immer ausgefeiltere Verkehrsüberwachungs- und Identifizierungssysteme wird, werden die Grenzen dieser technischen Lösungen deutlich. In dieser Masterarbeit stelle ich ein Framework für wallet-basiertes Identitätsmanagement von smarten Fahrzeugen vor, um einige Herausforderungen der traditionellen Ansätze zur Fahrzeugidentifikation in modernen Stadtgebieten zu bewältigen. Indem ich die Architektur des Frameworks vorstelle, die alle beteiligten Akteure enthält, sowie die Prozesse, die notwendig sind, um das Fahrzeug- und Fahreridentifikation zu ermöglichen, zeige ich einen alternativen Ansatz für die Fahrzeugüberwachung in Smart City Szenarien auf. Um in dieser Arbeit wissenschaftliche Genauigkeit zu gewährleisten, wende ich die iterative DSR Methodik an, bei der das Framework unter Berücksichtigung seiner Anforderungen und Design Objectives entworfen, durch Experteninterviews evaluiert und dann überarbeitet wird, um die neu gewonnenen Erkenntnisse einzubeziehen. Abschließend zeige ich die wichtigsten Ergebnisse des ausführlichen Evaluierungsprozesses, die Vorteile der Verwendung dieses Frameworks für die Fahrzeugidentifikation in der realen Welt und die verbleibenden Herausforderungen, auf denen zukünftige Forschungsarbeiten aufbauen können.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACDC	Authentic Chained Data Containers
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
BT	Bluetooth
CA	Certification Authority
CCZ	Congestion Charge Zone
CLI	Command Line Interface
DAPS	Dynamic Attribute Provisioning Service
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DMV	Department of Motor Vehicles
DO	Design Objective
DP	Design Principle
DSR	Design Science Research
DTM	Dynamic Trust Monitoring
eIDAS	electronic IDentification, Authentication and trust Services
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IAM	Identity and Access Management
ICT	Information and Communication Technology
IM	Identity Management
IIoT	Industrial Internet of Things
IoT	Internet of Things
IS	Information Systems

ITMS	Intelligent Traffic Management Systems
LEZ	Low Emission Zone
NFC	Near Field Communication
OCR	Optical Character Recognition
PKI	Public Key Infrastructure
PoC	Proof of Concept
PUFs	Physical Unclonable Functions
RFID	Radio-frequency Identification
SSI	Self-Sovereign Identity
TLS	Transport Layer Security
MITM	Man-in-the-Middle
QEAA	Qualified Electronic Attestation of Attributes
QTSP	Qualified Trust Service Provider
UI	User Interface
VC	Verifiable Credential
VSAT	Very-small-aperture Terminal
V2X	Vehicle-to-Everything
WAN	Wide Area Network
W3C	World Wide Web Consortium
ZKP	Zero-Knowledge Proof

1 INTRODUCTION

It comes to no surprise, that the rapid technological advancements in almost every aspect of our modern lives has already lead to a widespread integration of interconnected IoT devices into the vehicles we drive as well as the urban environment they move in. Equipped with numerous sensors, microcontrollers, and wireless transmitters, these smart vehicles, whose share on the road is predicted by PwC to rise up to 97 % in the US and up to 93 % in Europe by the year of 2035 [34], shape our cityspace today. And even our cities themselves follow the increasing worldwide trend of implementing "smart" concepts [10, 39], such as intelligent street lamps [52], connected traffic lights [29], or smart parking meters [43], to improve the quality of live for their citizen, enhance their efficiency, or various other use cases. With these new technologies available, it becomes apparent that a new paradigm of Vehicle-to-Everything (V2X) interaction between the smart vehicles and their city environment emerges quickly.

However, not only do modern cities change regarding their installed infrastructure or traffic participants, but also in terms managing them. With an increased demand for Low Emission Zone (LEZ) (see fig. 1.1), restricted parking spaces, residential areas or high congestion charge areas, [1] major cities around the world, resort to widely used traffic monitoring systems to identify individual vehicles and their drivers when they enter these restricted areas [19]. Unfortunately, the prevalent systems for vehicle identification have several drawbacks regarding, data privacy, environmental conditions, and accuracy, as the primarily rely on Automatic Number Plate Recognition (ANPR) using Optical Character Recognition (OCR) [19].

Motivated by these aforementioned points, I use this master's thesis to addresses the research question: How can smart vehicle identification be improved by using wallet-based identity management? Decentralized wallet-based identity management, sometimes referred to as Self-Sovereign Identity (SSI), is the concept of users managing their own credentials without or only minimal central authority [33]. Using wallet-based identities to realise decentralized identification, authentication or authorization scenarios lies in the very nature of this technology, combining it with the concept of driving smart vehicles

Figure 1.1: Traffic sign informing about a camera monitored LEZ in Glasgow [15].

able to communicate with IoT devices in modern infrastructure, however opens up completely new and complex questions to be answered. Very little research is done yet in this cumulative field between IoT, smart vehicles and infrastructure and identity management, which is why this thesis tackles the challenge of designing a novel framework by leveraging the individual technological advancements to create an improved vision of urban vehicle identification. A vision which incorporates the possibilities of user-centric, interoperable and yet privacy preserving nature of modern technology. As my goal for this framework is, to make it a valuable contribution to the scientific community, I follow the rigorous iterative DSR methodology for creating Information Systems (IS) artefacts, to ensure a high quality outcome, on which can be build in future research [32].

After this introductory chapter sets the stage for a comprehensive exploration of the challenges and opportunities in the design and evaluation of an identity management framework for smart vehicles, I will delve deeper into the existing literature, expound on the theoretical foundations of IoT, smart vehicles and infrastructure, and identity management, in the subsequent chapter 2, highlighting their relevance and applicability in the context of vehicular environments. Moreover in chapter 3, I present the details of the DSR research methodology employed for development and evaluation of the aforementioned framework to ensure the necessary scientific rigor. After I give an overview on the current pressing challenges regarding the devel-

opment of identity management frameworks in urban environments in chapter 4, I derive the necessary requirements and Design Objective (DO) for the evaluation of the framework in chapter 5. Moreover, I will explain in detail the design considerations, architectural elements and procedural steps of my proposed framework, demonstrating how it can effectively cater to the demands of wallet-based identity ecosystems in a smart city context in chapter 6. Subsequently in chapter 7, I present the procedure and results of the conducted evaluation to discuss the incorporation of the key statements, from the interviewed experts, into the final framework. I assess the framework's benefits for its users and the challenges that still need to be overcome in the penultimate chapter 8, while deriving more abstract key insights from it for future research to build upon. Ultimately I draw my final conclusions and implications for future contributions in this research area in chapter 9. Added in the appendix, the utilized interview guides (Appendix A), the complete transcripts of all conducted interviews (Appendix C) and the interview coding used to assess the gained qualitative data (Appendix B), can be found.

2

THEORETICAL BACKGROUND

Because this thesis touches the three research areas of IoT, Smart Cities, and wallet-based identity management, I begin with delving deeper into the theoretical understanding of these topics, to build a sufficient knowledge base as a strong foundation for development of the framework later on. This chapters purpose is therefor threefold. I define the terms and key concepts necessary for a basic comprehension in each of the aforementioned research areas. I present the current state of research as well as implemented real world usage. And lastly I illustrate how all three of these fields, can complement each other within the context of smart cities and smart mobility.

2.1 INTERNET OF THINGS AND SMART VEHICLES

The first concepts of IoT were already discussed as early as 1991 by researches like Mark Weiser. In one of his papers, Weiser described "*Specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence*" [50]. His definition already describes well what we today commonly understand as the IoT: A system that "*facilitates the machines and objects to communicate,compute and coordinate with each other*" [7].

Recent improvements in the areas of networking technologies, processing power and energy efficiency, make it possible for basically all kinds of modern devices to implement the common interfaces for network communications and connect to, public or private, networks. Their areas of application are just as varied as their design and purpose, which lead to the rapid increase of globally used IoT devices from 3.6 Bn in the year 2015 to 14.4 Bn in 2022, as mentioned in the *State of IoT - Spring 2023* report [26]. In many areas like manufacturing [36], healthcare [22], agriculture [23], transportation [8] and (home) automation [14], IoT devices play a vital role for numerous use cases.

Key components of IoT systems

Due the fast evolving field of IoT, a variety of attempts from expert to find one uniform taxonomy or categorization of IoT systems remained

unsuccessful. One way of categorizing modern IoT systems however, is by subdeviding them into the five key components (see fig. 2.1), the *Thing / Device* itself, the connection *Gateway*, the *Cloud*, *Analytics*, and the corresponding *User Interface (UI)* [37]. Like the name suggests, things or devices themselves are important versatile components in the IoT, for they are either a sensor measuring data or an actuator performing an action in the physical world. To establish a bidirectional connection between the various things and the internet, a gateway component is often used within the closed IoT network. The cloud component in IoT systems serves as a storage and processor of any amount of data that is gathered by the sensors of the thing. It is mostly installed on online servers as they can utilize more storage capacity and performance than the small constraint physical devices. To make sense of the data on the cloud storage, Analytics components play a vital role, by processing the data and acting according their programming. The UI of IoT systems can vary between minimalistic, such as simple Command Line Interface (CLI) with few text based commands and sophisticated application with graphical interfaces and many usage options for an intuitive user experience.

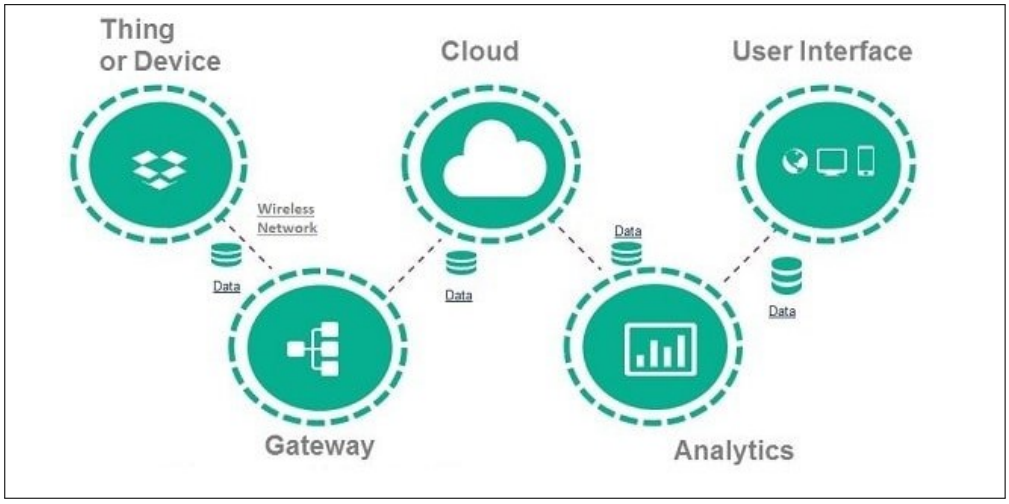

Figure 2.1: Example of a service-oriented IoT architecture with its individual components and layers [37].

Connecting multiple IoT devices together to form a, mostly wireless, network is one of the core principles in IoT [27]. Due to the versatile nature of these devices, numerous forms of network topologies (see fig. 2.2), from completely distributed mesh networks, over federated connected hubs, to classic star-topologies, can be implemented. However physical constrains like range, antenna voltage, or number of devices are always to be taken into account when considering the

right type of network and transmission protocol for ones use case [17]. Common protocols for communication are Bluetooth (BT), Near Field Communication (NFC), or WiFi each coming with its own benefits and drawbacks [27].

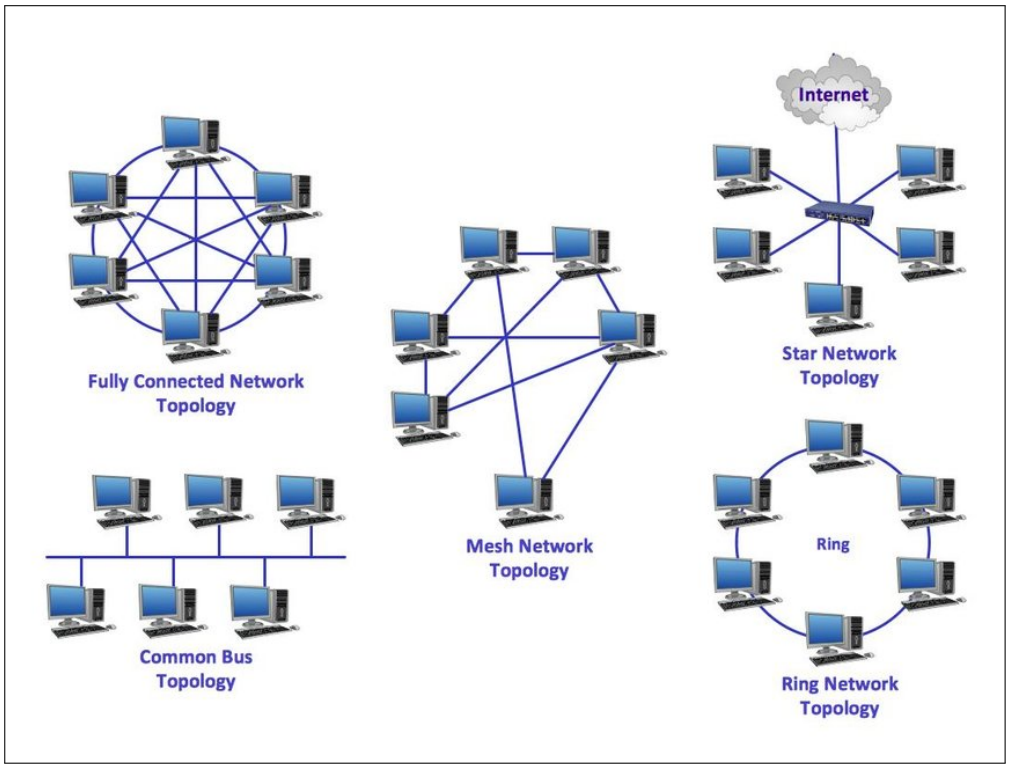

Figure 2.2: Possible network topologies for IoT devices [17]

Dependent on the use case, the different components of IoT systems are often assigned to one of several distinct architectural layers, according to their purpose within the system (see. fig. 2.3) [7]. The layers themselves are often times only of abstract nature, yet help to order related components together in complex system architectures.

Implementing IoT in Smart Vehicles

IoT devices can be seamlessly embedded within, so called, smart vehicles, as seen in figure 2.4, allowing new ways of connectivity and data driven analytics to improve the driving experience for the vehicle driver and passengers [25]. Sensors like cameras or radar capture a multitude of data points from the vehicle's surroundings, monitoring road conditions, traffic patterns, and even driver behavior [25]. The numerous data streams of these sensors are then transmitted to one

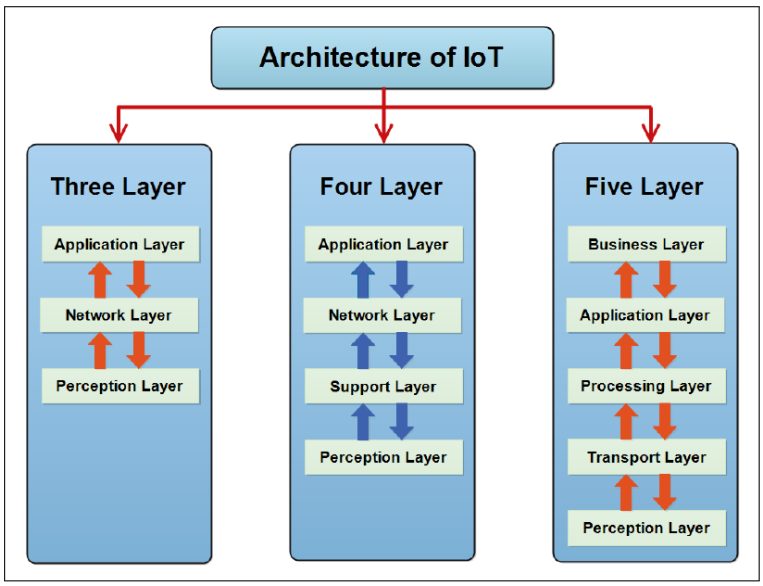

Figure 2.3: Overview possible architecture layers of IoT systems [7].

or more of the vehicle's central processing unit or even to a cloud component online [25].

IoT devices implemented in smart vehicles enable the creation of a completely novel interconnected network, not only to other cars, as Vehicle-to-Vehicle (V2V) communication, but also to pedestrians (V2P), the infrastructure itself (V2I) or others [21]. The resulting V2X ecosystem has the potential to set new standards in the way smart vehicles move in cities.

Identity Management in IoT

The heterogeneous nature of IoT devices and networks raise fundamental challenges in regard of identity, device security, and trust [45]. Every single device within the network can potentially be vulnerable to security exploits and in consequence serve as an attack vector to every other connected component and with an increasing number of devices within a network, deploying security updates, managing permissions, or detecting single compromised devices becomes a difficult task [45]. Without reliable ways of identifying and authenticating trustful devices, malicious actors could also gain access to a IoT systems by spoofing identifiers or messages [49]. Administrators of IoT networks oftentimes employ various protocols and authentication mechanisms to establish a secure identity of devices to safeguard exactly this data integrity, and control access [40]. However with the

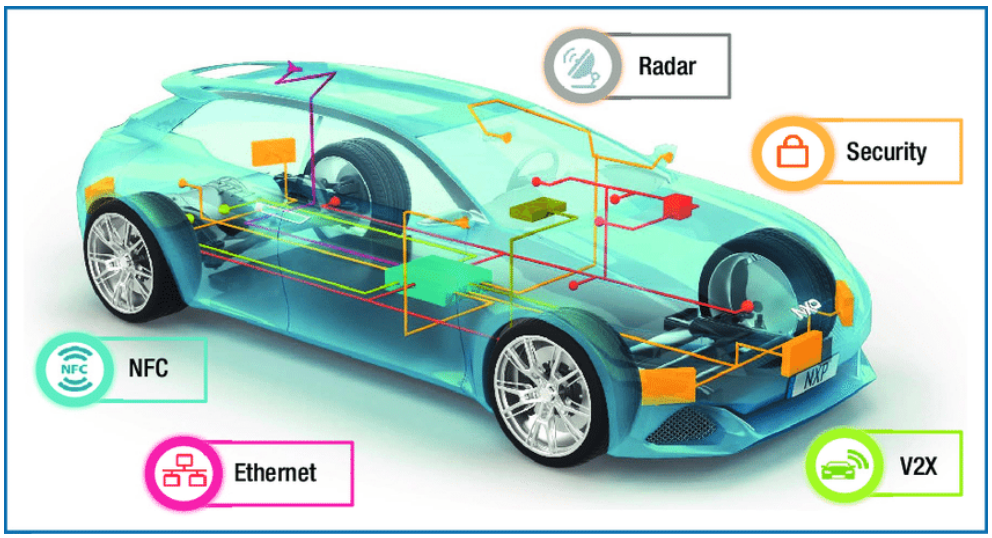

Figure 2.4: Components of a Smart Car for sensing and communicating with its environment [28].

rise of wallet-based identity management systems, new possibilities for decentralized IoT identities emerge.

2.2 SMART CITY INFRASTRUCTURE

While it is unclear among expert circles, when and where the term "smart" city was coined the very first time, today various definition and explanations are used simultaneously interchangeable [31]. Even as it now becomes apparent, that many slightly different definitions of smart cities exist in the research community, their main goal and purpose is similar: utilizing modern technology to improve the quality of living for every resident by tackling aspects like sustainability, pollution, traffic, efficiency, or others [5]. And as the level of urbanisation worldwide is rapidly increasing up to over estimated 68 % by the year 2050 [48], aspects to tackle with technology are sufficiently available.

Key concepts of smart cities and smart mobility

Several aspects can be described as components of a smart city, as seen in fig. 2.5, Savithramma et al. list *Smart Economy*, *Smart Governnance*, *Smart Living*, *Smart People*, *Smart Environment*, and *Smart Mobility* in their paper as the six main components, all of which have in common the utilization of modern technology with the goal of improv-

ing [43]. Smart Economy entails improved entrepreneurship to drive economic growth and job creation within the city, while Smart Governance utilizes technology to simplifying official visits by increasing transparency, citizen participation, and efficient public service delivery. Improving residents' quality of life through new technological solutions, is called "Smart Living", in contrast to improving their education or vocational training, which is called "Smart People" The components of Smart Environment and Smart Mobility partially overlap, as the former focuses on environmental sustainability, integrating eco-friendly practices and energy consumption, and the latter on transport systems, intelligent traffic management, lowering emissions and smart infrastructure. All of these six components form a coherent frame for smart city related technologies to focus their effort on.

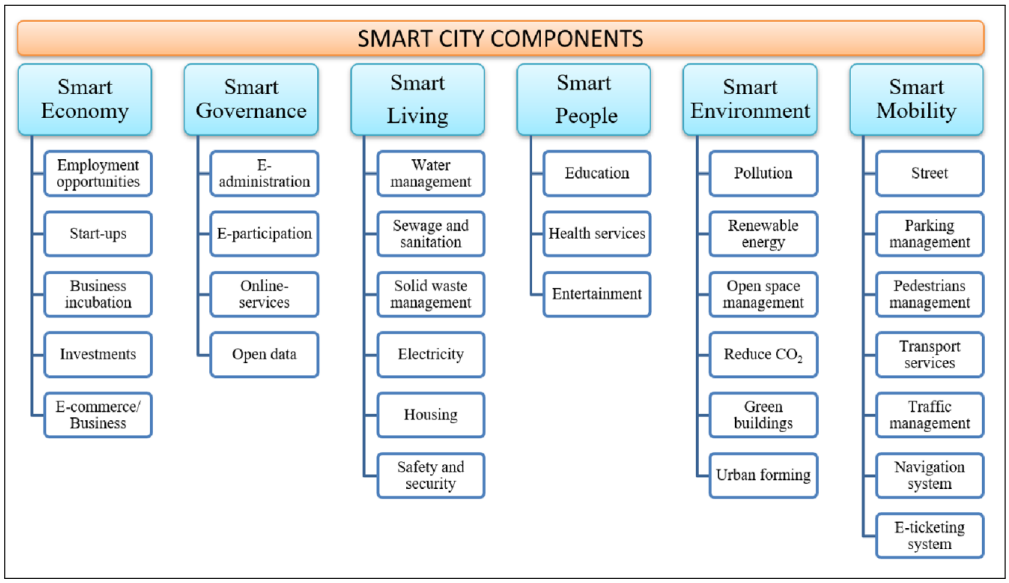

Figure 2.5: Overview of the six different Smart City components [43].

Identity management in smart mobility

Identity management plays a crucial role in the context of smart cities, where novel technological advancements purposefully introduced to be widely adopted in the urban landscape [10]. With various interconnected services and systems deeply embedded in the daily smart city life and official processes, the citizens are most likely to proof their identity on regular basis. Effective identity management ensures the privacy, security, and seamless interaction of citizens with each other, automated systems and official institutions and makes the development and deployment of trusted, secure and efficient Identity and

Access Management (IAM) frameworks all the more important [33].

2.3 WALLET-BASED IDENTITY MANAGEMENT

Wallet-based identity management (often referred to as SSI) is a user-centric concept where personal data of a user is stored and managed by himself in software wallets instead of a centralized server as often used in prevalent IAM architectures [33]. Key element difference between this approach and the use of a centralized IAM system is the replacement of a single central trustworthy authority, and the therefore emerging hierarchy, with an also decentralizable trust anchor.

Key roles of wallet-based identity architectures

The entities in a wallet-based identity management system can be identified by their roles as (Credential) Holder, (Credential) Issuer and (Credential) Verifier. While these roles can sometimes be held by the same entity, each of them serve a distinct purpose within the identity management architecture. Figure 2.6 illustrates how these key roles relate to each other so issuing and verification of Verifiable Credential (VC) can work. The holder receives a VC from an issuer and keeps it stored securely in his secured wallet application for himself on his device. VC are digital representations of qualifications, attributes, or other personal information that can be independently verified by verifying entites. These credentials enhance privacy and security, as they enable individuals to selectively disclose specific information without revealing unnecessary details. To issue a VC the issuer, often an public or governmental institution (e.g. a Qualified Trust Service Provider (QTSP) [11]), creates a digital VC containing the subject's information and digitally signs it and transfers it to the holder via a secure connection. Verification of these VC occurs when the holder chooses to share their credentials with a verifier, which could be an employer, service provider, or any entity requiring proof of specific attributes. The verifier, without needing to access a centralized database, can verify the authenticity of the VC by checking the issuer's digital signature and relying on the verifiable data registry as decentralized trust infrastructure, Distributed Ledger Technology (DLT) or other cryptographic mechanisms.

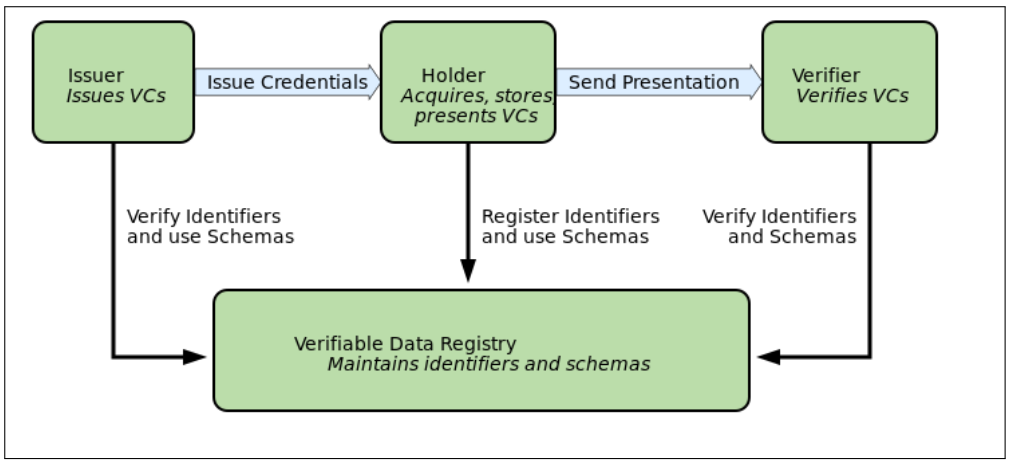

Figure 2.6: Basic overview of the three key roles in wallet-based identity systems and their relationship to each other as defined by the W3C [46].

Identity Management with Wallet-Based Identities

Wallet-based identity management offers a paradigm shift in how identities are defined, utilized, and controlled compared to the conventional methods. Identities, whether human or of a device, are no longer confined to centralized databases, instead, they are encapsulated as Decentralized Identifier (DID) within the user's cryptographically secured wallet [33]. As DID are unique globally resolvable identifiers by design and VC meant to be issued and verified without a central governing authority, standardization plays a crucial role in the success of wallet-based identity management and its broader adoption. Collaborative efforts across industries and organizations have led to the development of standardized protocols, such as for DID [47] and VC [46]. However, since wallet-based identity management is still a very young concept, more efforts for standardization are needed in the future to cover even more use cases for interoperability.

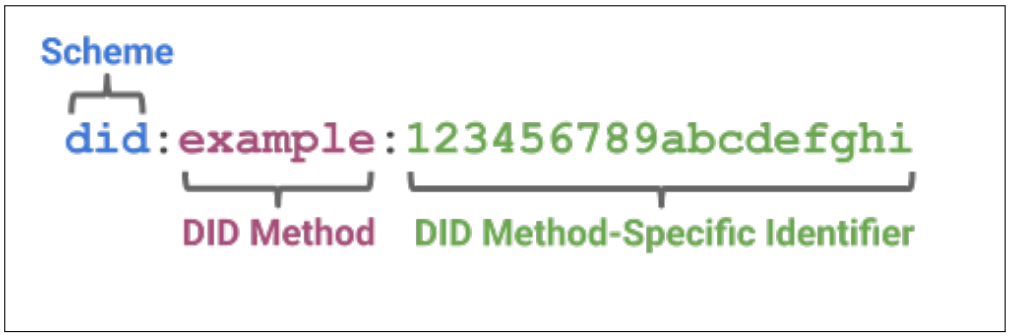

Figure 2.7: Example of the segments of a DID as defined by the W3C [47].

Delegation of VC enables users to grant temporary access to specific credentials to trusted entities. This is accomplished by generating a cryptographic proof of the delegation, allowing the third party to access and verify the specified credential without exposing the entire wallet's contents [44]. Should a VC, on the other hand, becomes expired or compromised, it can be revoked by the issuing party and verifiers are able to check the VC revocation status during the verification process [33].

Implementations and Use Cases of Wallet-based Identity

Wallet-based identity management holds immense potential for a wide range of use cases, through countless application areas. Several real-world scenarios for personal identity wallet applications have already been implemented or are currently being developed [42]. In the broader context of smart cities, potentially use cases for urban residents, range from improved interaction with public administrators to e-ticketing systems for public transport [35, 43]. Even for the use on smart vehicles, wallet-based identity management has some benefits, compared to conventional methods, as this thesis will show in the next chapters.

3

DESIGN SCIENCE RESEARCH APPROACH

Now that I laid out the theoretical foundations of the relevant topics of this thesis in the previous chapter 2, I explain the methodology I use to conduct my research. For this, I describe how I apply Hevners et al. IS Research Framework in this thesis, to ensure the necessary scientific rigor and relevance to produce a high quality IS artefact. Subsequently I also go into detail how the iterative DSR process of Peffers et al. helps me when developing the identity management framework architecture and its processes.

Hefner et al. introduce their Framework for IS research based on insights and paradigms from behavioral science and design science, to help with the development of IS artefacts to solve specific research problems [18]. The form and type of said artefact is not predefined and varies depending on the problem it tries to solve. Typical artefacts regarding information technology system can take for form of source code, documentation, circuit diagrams, Proof of Concept (PoC), or other technical designs. Regardless of its form, an artefact needs to be relevant enough for the so called *business need* to be worth implementing. To also ensure scientific rigor of the artefact, it needs to be based on previous *applicable research* and build upon it.

Applying this research framework to my thesis leads to the development of an artefact in form of a wallet-based identity management framework. Improving of current city identity management systems serves as a business need for this artefact to be relevant to. Ensuring the rigor of the artefact is its foundation on previous knowledge base on the hand and the execution of the DSR process on the other.

In figure 3.2, I also show the application of Peffers et al. DSR process on my thesis, as a rigorous procedure for developing an artefact and refine it iteratively until it meets a high enough quality for publication [32]. During the first, of six, step of *Problem Identification*, I evaluate the current state of smart vehicle identity management and assess the drawbacks and challenges, the established systems have to face, to illustrate the relevance of my research in this area. For the *Definition of Design Objectives* afterwards, I elaborate the necessary requirements for comparable frameworks and derive DO out of it. The

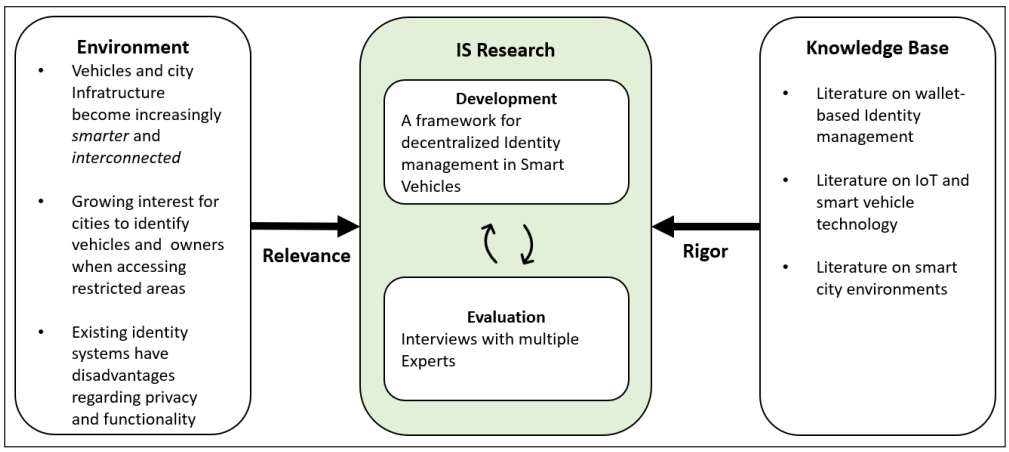

Figure 3.1: Applying the Design Science Research Framework on my thesis.

choice and iterative refinement of DO is important, as their fulfillment is a key aspect for later evaluating the current state of the framework. In the subsequent *Design and Development* step, I create the first iteration of my IS artefact, a framework architecture to use wallet-based identity management with smart vehicles within smart cities. Literature resources on the topics of wallet-based identity management, IoT and smart vehicles are as used as documentation of implemented real world systems. A *Demonstration* of this first iteration of the framework is done by presenting it to several experts from different fields during conducted interviews. Each entity, component, and process between them are introduced and explained via presentation slides. To *Evaluate* the artefact, I gather the insights of the expert interviews, by transcribing the dialogues and apply a coding system to quantify the qualitative data. With these insights, I am able to put the expert assessments into context and evaluate the frameworks architecture, fulfillment of DO and actual real world feasibility. By reiterating the process steps afterwards, the notes and statements of the experts are also incorporated back into the framework and DO, to refine or correct all wrong or undefined aspects of it. I repeat these last four steps for a second iteration before lastly deciding to start the *Communication* step by writing this thesis.

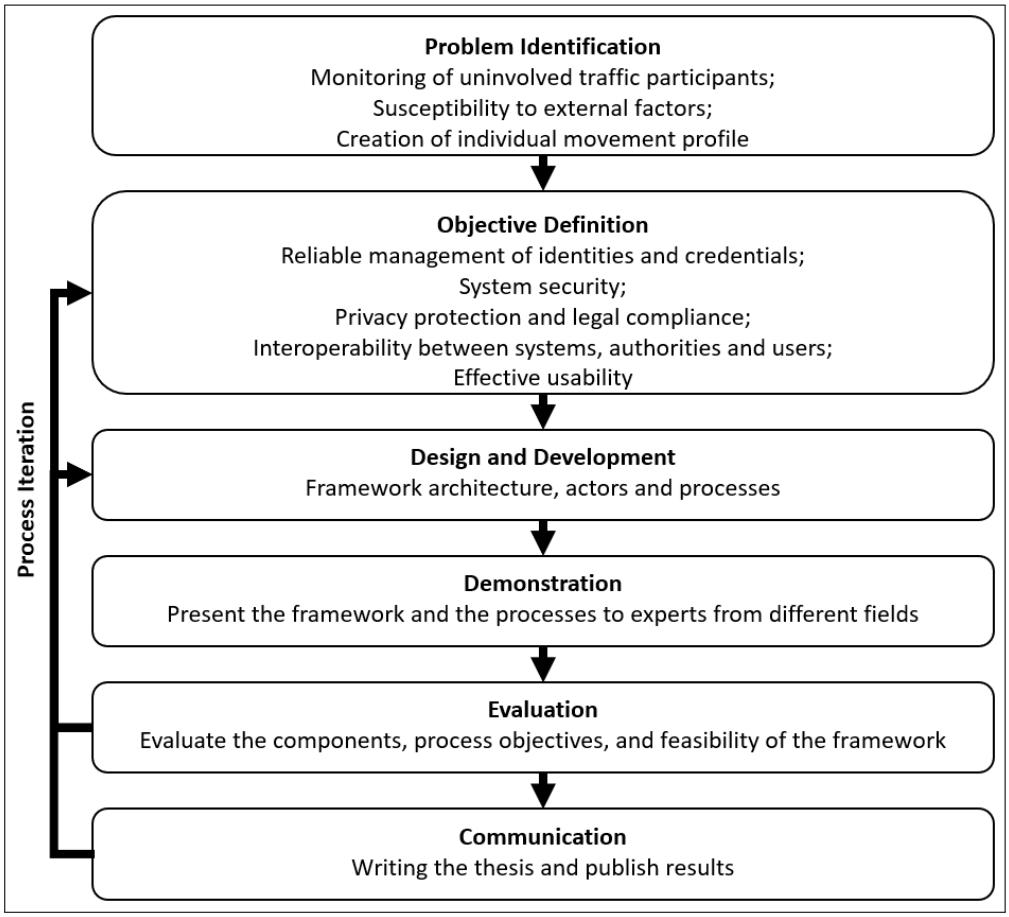

Figure 3.2: Steps of the iterative DSR process applied to this thesis.

4

PROBLEM DEFINITION

Now that I explained the theoretical background in chapter 2 and the research methodology I use in chapter 3, I will go into detail of the research question addressed in this thesis and its applicability in real world scenarios. For this I describe my process of deducing a research question of relevance from the current state of research and how I derive the challenges that motivate the development of my new identity management framework.

As I describe in chapter 2, the increasing global trend of making cities smart has a big transformative effect of inter-city mobility as a whole. Benolo et al. identify in their work several possible targets for technology to aim for when implementing smart mobility approaches in these newly emerging smart cities and describe in their developed taxonomy, the 52 most relevant actions that have a crucial role in it [5]. After asserting these smart mobility use cases, I rate them based on categories like *how high is the potential use with wallet-based identity management*, *how high is their intensity of Information and Communication Technology (ICT) and IoT adoption*, and *are enough benefits for smart mobility fulfilled to be relevant*, to find out which of the suggested use cases is the most fitting for my thesis. This assessment finally leads me to the remaining issue of *Control systems for access to reserved areas*, as it has numerous potentially overlapping topics with managing identity, while at the same time has a high ICT adoption, and multiple direct benefits for smart mobility implementations.

Combining the topic of reserved area access with identity management technology, quickly results in the follow-up question on how access to those restricted areas is currently managed in modern cities? Prevalent technological solutions include inductive loops in the road, regularly sending the vehicles Global Positioning System (GPS) coordinates, or using cameras to monitor the street.

However many of these monitoring solutions to identify vehicles and, if necessary, manage their access come with severe drawbacks, ranging from violating the privacy of uninvolved traffic participants, over susceptibility to changing external influences (e.g. environment, setup, quality of OCR software), up to potentially creating movement profiles [19].

These aforementioned drawbacks of currently widely prevalent identity management solutions make the concluding research question for this thesis, how smart vehicle identification can be improved by using wallet-based identity management, all the more relevant.

5

DESIGN OBJECTIVES

After analysing the drawbacks of the currently prevalent methods of traffic access management and the challenges to overcome them in chapter 4, I now want to derive DO for my framework off of them and assess their necessary requirements.

As I described in chapter 3, the definition of DO are key points when evaluating the framework. Additionally to the feasibility of its overall architecture, the framework is evaluated and revised, based on the fulfillment of the DO in chapter 7. After analyzing the challenges in current traffic identification systems in the previous chapter 4, I derive the five DO *Reliable Management of Identities and Credentials*, *System Security*, *Privacy protection and compliance*, *Interoperability between participants*, and *Effective usability*, to be met by the framework. I also show an overview of these DO in table 5.1. Just as the framework architecture itself, the DO are also subject to the evaluation process and undergo the iterative evaluation and refinement.

OBJECTIVE 1: RELIABLE MANAGEMENT OF IDENTITIES AND CREDENTIALS

In its core, the framework needs to be able to effectively manage and authenticate the different identities of all participants in a consistent and trustworthy manner. This DO is crucial for maintaining the integrity of every issuing institution, smart vehicle, owner and verifier and their individual attributes.

Requirements:

1. **Ensuring trust between Participants**:
   Trust between all participants of the framework is existential for identity management [33]. As the issuer represents a public institution, existential service or manufacturing company its identity must be easily and reliably checkable when verifying its issued VC. The same applies to any verifying entity, to rule out malicious attackers, and the VC holders that need to authenticate themselves before receiving a VC.

2. **Decentralization**:
   For a wallet-based identity framework to reliable manage identities, it must make use of its properties for decentralized managed identity wallets and agents [33].

3. **Unique identifiers**:
   It is important for every participating entity to have an individual unique identifier to distinguish individual actors and devices from each other when issuing or verifying VC [33].

4. **Processing of verifiable attributes**:
   The specific attributes that are attested to both the individual user and the vehicle he owns or drives with must be in a form that allows them to be issuable, revocable, delegatable and verfiable [33].

OBJECTIVE 2: SYSTEM SECURITY

Implementing robust measures and strategies to safeguard the framework against a wide range of threats, vulnerabilities, and unauthorized access, plays a vital in any digital system in the current age. This objective is essential for ensuring the integrity, confidentiality, and availability of sensitive identity and VC data on all systems and sub components within the framework as well as their transmission between the frameworks entities.

Requirements:

1. **Encrypted data storage and transfer**:
   The protection of stored as well as transmitted data requires the utilization of modern encryption technologies to prevent sensitive information like identity or VC details from unauthorized access and interception [41].

2. **Robust transmissions**:
   Connections between the different participants of the framework need to be reliable, secure and resilient against interference, so that VC can be transmitted without disruptions, be it intentional or unintentional [41].

3. **Authentication of issuers, holders, and verifiers**:
   There needs to be a way to ensure the authenticity of all participants when interacting within the framework. Especially before

issuing VC from an official institution to a user and when requesting a proof from a verifier [41].

4. **Tamper proof identifiers**
   As the unique identifiers of all participants are crucial for the issuing and verification processes of the framework, they must not be easily duplicable or modifiable, so that malicious attempts spoofing another identity by cloning the corresponding hardware or software component is not possible. This is usually done by utilizing Physical Unclonable Functions (PUFs) in vehicular security systems [4].

OBJECTIVE 3: PRIVACY PROTECTION AND LEGAL COMPLIANCE

Since the VC issued to the owner and the vehicle can contain information of very sensitive nature (e.g. address details, health status, etc.), measures that protect this user data are important not only to be compliant with local laws and regulations, but also to preserve the users privacy. This ensuring and preservation of user trust can only be achieved through strong system security measures (see DO 2), as for example the confidentiality of these information requires reliable encryption and authentication [16].

Requirements:

1. **Legal Compliance**:
   Ensuring that the framework aligns with relevant privacy laws and regulations for its operational location, such as the General Data Protection Regulation (GDPR) in the European Union or similar data protection laws in other jurisdictions, if available[16].

2. **User- and Meta-Data Minimization**:
   Collecting and storing only the minimum amount of data necessary for the framework's operation, limiting the collection of personal information and transmission metadata to what is essential and relevant to the specific transaction [16].

3. **Explicit User Consent and selective disclosure of information**:
   User consent must be obtained and be easily revocable before personal information is processed within the framework. The user must always be able to make informed decisions on what data is shared when it comes to verification [33].

OBJECTIVE 4: INTEROPERABILITY BETWEEN SYSTEMS, AUTHORITIES AND USERS

The ability of different actors within the framework to seamlessly communicate, exchange data, and work together effectively is of particular importance in such a heterogeneous environment such as smart cities. This interoperability is crucial for ensuring that various smart vehicles, users, and platforms can interact and collaborate within the identity framework, regardless of their used technologies or manufacturers. Achieving this interoperability helps preventing centralized silos, fosters a more connected and efficient data exchange, and enables new third-party participants to easily join ecosystem [9].

Requirements:

1. **Standardized communication protocols and data formats**:
   Using established standards and formats, that are widely recognized and accepted within the industry, is required to promote consistency on as many abstraction layers as possible, to ensure that all participating entities can understand and process information consistently and additional frameworks or regulations can be further join the ecosystem [51].

2. **Nonexclusive system support**:
   The framework itself as well as its components must be system agnostic, so that its functionality is not exclusively usable on certain vendor specific soft- or hardware systems or programming languages [9].

OBJECTIVE 5: EFFECTIVE USABILITY

To actually be widely adopted in real world scenarios, it is important to create a framework that offers a high level of usability, empowering users to interact with the system effortlessly, while also considering the complexities of scaling to accommodate a larger user base and providing interfaces that are intuitive and user-friendly, so that all participants can interact with the framework smoothly and without unnecessary complications.

Requirements:

1. **Minimal complexity**:
   As large distributed systems tend to become complicated, it is

important to reduce their complexity as much as possible, to increase overall transmission performance, maintainability, fault tolerance, security, and recoverability after errors [3].

2. **Efficient scaling**:
   The framework must scale well with an increasing number of issuing institutions, verifying infrastructure devices, users, and vehicles, while still being responsive, usable and keeping transmission latency low, to ensure its widely usage [30].

3. **Intuitive user interfaces**:
   All users that interact with the technical components of the framework need have UI that allows them to control, configure and monitor the wide range of events and interactions that are happening around their system. Only with an intuitive UI, with meaningful control elements, understandable system messages and good maintainability, the acceptance of such a framework is possible [6].

#	Objective	Description
1.	Reliable management of identities and credentials	Manage the identities, attributes and credentials of the various framework participants.
2.	System security	Ensuring a secure usage of all framework functions on all involved systems.
3.	Privacy protection and legal compliance	Preserve the privacy of all sensitive user information while staying compliant with local laws and regulations.
4.	Interoperability between systems, authorities and Users	Be interoperable and open to all participating and new systems by utilizing available standards and protocols.
5.	Effective usability	Facilitate user adoption and efficient use in fast scaling real world scenarios.

Table 5.1: Overview of the identified design objectives and their description.

6

FRAMEWORK

With the DO defined in the previous chapter 5, I use this chapter for a detailed definition and explanation of my created wallet-based identity framework after incorporating the findings of the expert evaluation. First I introduce and describe the architecture, its interacting entities and their sub-systems, and the flow of information to explain their distinct roles within the framework. I also give insights about the extended version of this architecture, where I add a definition for the passenger entity to the framework to demonstrate additional use cases. Following this, I go into detail about how the different processes of VC issuing, delegation and verifying work within the framework to ensure a smooth and secure operation.

6.1 FRAMEWORK ARCHITECTURE

The developed architecture for this framework can be subdivided into the base structure and, build upon, an extended structure. This division is made to better differentiate between the well established procedure of issuing, holding and verifying between a public institution, a vehicle owner and the infrastructure devices (see 2), which is prevalent in many wallet-based identity frameworks, and the involvement of additional passengers that delegate their VC as well to the smart vehicle.

Base Architecture

The base architecture consists of six distinct entities that communicate with each other. As I show in Figure 6.1, each of these six participating entities have a distinct role and consist of internal sub-components for specific tasks.

Public institutions act as an issuer entity for VC, which work as digital representations of personal information or permission that can be securely stored and shared with identity wallet applications. This institutions may be government agencies, health insurance companies, or other private companies, that are able to provide a vehicle owner with individual VC about his residential address, existing disability, or access authorization. Under consideration current European Union regulations like electronic IDentification, Authentication and trust Ser-

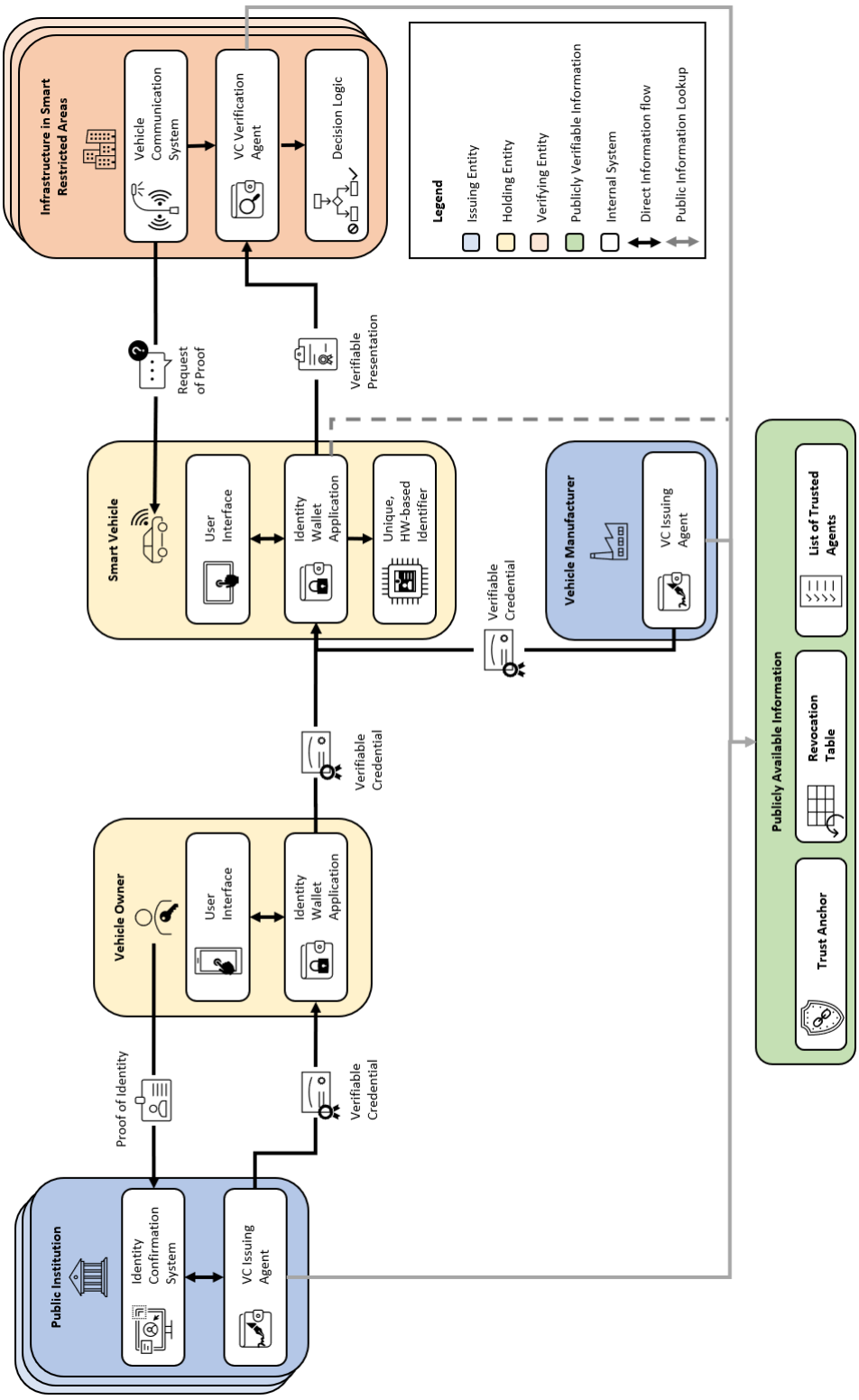

Figure 6.1: Architecture overview of the wallet-based identity framework for traffic access management.

vices (eIDAS), a QTSP could fit this role [12]. The institutions play a crucial role in ensuring the accuracy and authenticity of the VC they issue. Mainly needed for the issuing process of a public institution, are two key sub-systems for identity confirmation and an agent for VC issuing. The public institution needs a reliable system for verifying the identity of a vehicle owner requesting a certain VC, to confirm that he is actually entitled to do so. This identity verification typically involves a combination of processes and technologies designed to ensure that the information provided by the individual aligns with the institution's stored records and predefined issuing criteria. As this system is responsible for confirming the identity of the credential holder, thereby it must make usage of reliable technologies like *ID Verification* (e.g. passports, ID cards, driver's licenses, etc.), *biometric verification* (e.g. fingerprints, facial scans, iris scans, etc.), or *multi-factor authorization* (e.g. sending one-time codes to the persons registered address, etc.). Only after this confirmation, the VC Issuing Agent actually issues the credential. The actual issuing of standardized, interoperable VC happens by the issuing agent sub-systems and sent to the vehicle owner. To confirm the issuer as trustworthy public entity, its identifier is also included in the public list of trusted agents.

The vehicle manufacturer is the entity responsible for producing the smart vehicle and equipping it with various digital systems and technologies. Similar to the public institutions, the manufacturer serves as an issuer of VC, but is able directly embed the relevant information into the vehicle at the manufacturing plant. These VC pertain to the model information, technical specifications, and other relevant attributes of the smart vehicle like a unique identifier for the specific smart car model and its manufacturing details, Information about the car's make, model, year, engine type, fuel efficiency, and other technical attributes, as well as environmental compliance data related to emissions and pollution standards. A issuing agent within the vehicle manufacturer's organization is a designated sub-system responsible for generating and digitally signing the verifiable credentials related to the smart vehicle. This agent ensures the accuracy, security, and integrity of the information being included in the VC. The manufacturer is also included in the list of trusted agents to ensure, that the issued vehicle specifications are from a genuine origin.

The vehicle owner assumes the role of a holder for the VC he gets issued by public institutions. His primary systems to make use of the framework are the UI and the identity wallet application. The UI is the visual and interactive component through which the vehicle owner in-

teracts with the identity wallet application. Due their prevalence, this most likely be via a smart device such as a phone, watch, or other connected devices. It provides a user-friendly way for the owner to access and manage his verifiable credentials by creating access to the identity wallet application. The identity wallet application is the software or (mobile) application used by the vehicle owner to store, manage, and share their verifiable credentials securely. This application acts as a digital container for the credentials and employs cryptographic technologies to ensure data integrity and privacy. The integration of the identity wallet application into the UI empowers the vehicle owner to manage their digital identity and credentials effectively. By having a clear and user-friendly interface, along with a secure wallet application, the vehicle owner is able to autonomously present, store, delegate, backup and restore his VC, as he likes. Utilizing open data standards and protocols, several identity wallet applications from different vendors can be interoperable on various devices.

Just as the vehicle owner himself, the smart vehicle also plays a role as a holder of VC, which are delegated from its owner onto its identity wallet application. Besides its ability to wireless communicate with other devices such as smart devices from its owner or passenger, the smart vehicle makes use of its internal V2X technology to communicate with its surrounding infrastructure. The UI within the smart vehicle enables the interaction between the vehicle's occupants - drivers as well as passengers - and the identity wallet application of the vehicle. This interface may be operable on a (smart) screen within the vehicle dashboard or be accessible on a separate external smart device. The identity wallet application within the smart vehicle is a sophisticated software component that manages the VC received from the owner and vehicle manufacturer. This application ensures that the vehicle's credentials are stored securely and can be shared in an individually configured manner with infrastructure devices. It is responsible for securely storing the delegated VC in an encrypted data wallet, manage the incoming VC delegations, configure the selective disclosure and automatic creation of verifiable presentations, as well as answering incoming proof requests. The vehicles unique hardware-based identifier is a distinct and unalterable identifier assigned to it and serves as a foundational component of the vehicle's identity, allowing it to be recognized and authenticated within the identity framework. The identifier is meant to be implemented in a tamper resistant and non-duplicable way, to prevent the theft of the smart cars identity. The integration of these three sub-systems within the smart vehicle, empowers the vehicle to manage and present its own VC as well as those

delegated by its owner securely when interacting with the smart infrastructure devices in this framework.

In the identity framework within restricted smart city areas, such as zones with controlled access or specific traffic regulations, the infrastructure devices like street lights or traffic lights play a critical role in enforcing access rules. Each of these infrastructure devices integrates sub-systems for "vehicle communication," "credential verification," and "decision logic." The vehicle communication sub-system within each infrastructure device registers approaching smart vehicles and facilitates communication with them, when they are nearby. This communication makes use of established IoT standardized protocols e.g. Radio-frequency Identification (RFID), Bluetooth, WiFi, etc., which enable the infrastructure to interact with vehicles and request relevant information for access control purposes. Is a wireless connection between a vehicle and an infrastructure devices established, identification and relevant VC can be established via a secure communication channel to ensure data privacy and prevent replay or spoofing attacks. Additionally, no actual information of the VC owner is transferred during the verification, by using Zero-Knowledge Proof (ZKP) for the proof request. The credential verification agent is then responsible for validating the verifiable presentation presented by the smart vehicle. The decision logic sub-system of the respective infrastructure device, reacts accordingly to the result of the verification process, afterwards.

Publicly available Information provides the basis of every issuing and verifying entity within the identity framework and thus play significant part in its real world application. This information must be accessible by every issuer, holder and verifier alike and consists of the VC trust anchor, revocation table and the list of trusted agents. A public trust anchor serves as cryptographic key or identifier that is widely recognized and accepted as a trustworthy source within the identity ecosystem. It ensures the validity of publicly issued VC, their schemas and definitions. A public revocation table contains information about credentials or entities whose trustworthiness has been revoked or invalidated. This table helps maintain the integrity of the identity ecosystem by ensuring that outdated or compromised credentials are not used. A public list of trusted agents contains information about entities that are authorized to issue or verify VC within the identity framework. This list is publicly available and centrally managed by a governmental authority to make it possible to verify the identity of entities issuing VC or sending proof requests to the smart vehicle. This public information greatly hampers, imposing as trustworthy en-

tity by malicious actors. As part of the eIDAS regulation, the European Union foresees such a list containing QTSP for each member state [11].

Extended Architecture

Extending the base architecture of the framework means adding another participant to in the form of a smart vehicle passenger to it. As seen in Figure 6.2, this new entity represents additional use case scenarios, such as car pooling or fleets, to the framework as a whole, as the smart vehicle now receives the VC of multiple different people delegated to it.

Same as the vehicle owner, the vehicle passenger is also considered a holder entity of VC. This passenger can have their own set of credentials that pertain to their identity, which can overlap or supplement those of the owner as they can also be issued by public institutions. Mirroring the capabilities of the vehicle owner, the passenger has the ability to interact with the smart vehicle via his UI and corresponding identity wallet application. His UI also serves as a central application to manage his identity wallet application. The identity wallet application of the passenger does not have to be the same as of the vehicle owner, as long as it implements the interoperable standards and protocols. However, delegating a VC from a passenger must come with certain limitations to prevent abuse or fraud, as a malicious actor could circumvent area restriction within a smart city by delegating his VC to multiple vehicles without actually being a passenger of them. To prevent this kind of exploitation, VC delegated by passengers must be either proximity bound, to ensure a person is inside the vehicle during verification, or bound to be stored only certain amount of time, before being deleted from the vehicle wallet.

The extension of the base architecture has the most effect on the smart vehicle itself. Whereas in the base architecture, the smart vehicle only stores the VC delegated by its owner, it now pools multiple VC from multiple delegating people. During a verification process with an infrastructure device, the presentation of any valid VC

6.2 IDENTITY MANAGEMENT PROCESSES

After explaining the entities partaking in the framework architecture in detail, I will now describe the processes of the framework to bet-

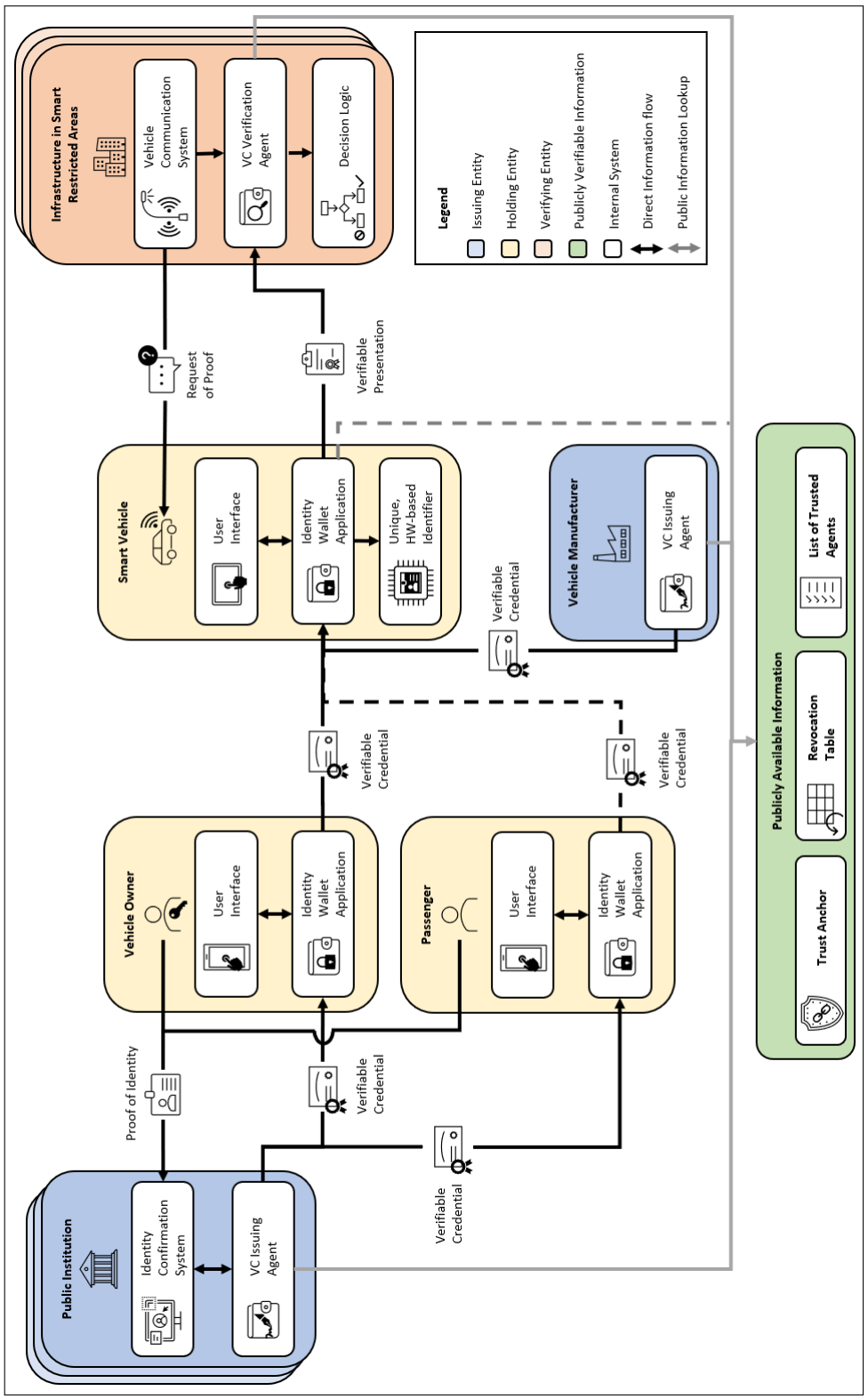

Figure 6.2: Architecture overview of the wallet-based identity framework extended for multi passenger usage.

ter elaborate the flow of information during connection establishing, issuing of VC, delegation between owner and vehicle and verification.

Issuing Process

Before issuing a VC to a vehicle owner a secure connection needs to be established, as shown in Fig. 6.3. The process begins with the vehicle owner providing physical proof of their identity to the identity confirmation system, which could involve presenting government-issued identification documents, biometric data, or other forms of identity verification. The identity confirmation system verifies the provided identity information by checking the authenticity of documents, comparing biometric data, or otherwise running checks against identity databases. Once the vehicle owner's identity is confirmed, the identity confirmation system triggers a request to the credential issuing agent to confirm that the identity verification process is complete and that the requested VC needs to be issued to the vehicle owner. The credential issuing agent generates a connection invitation to establish a secure communication channel between the agent and the vehicle owner's identity wallet application. Importing this connection invitation can happen on multiple ways such as QR codes, RFID tags of sent hyperlinks. After the vehicle owner receives the connection invitation, his identity wallet application establishes a secure connection with the credential issuing agent.

With the secure connection in place, the credential issuing agent can now issue the VC to the identity wallet application of the vehicle owner, see Fig. 6.4. The issuance of the VC is based on schemas and definitions stored on the publicly available trust anchor. If the VC supports revocation information or expires, those information is also set up by using the public revocation table. The vehicle owner's identity wallet application receives the offer to accept the VC, which is automatically confirmed to receive the actual VC directly afterwards. Once received, the VC is securely stored within the identity wallet's encrypted storage and can be subsequently used whenever identity verification is necessary.

Credential Delegation Process

Delegating a VC from the vehicle owner to the smart vehicle, as shown in Fig. 6.5, begins with the vehicle owner initiating the delegation process via the UI on both, his personal smart device and his vehicle. During this initiation, the smart device and the smart vehicle pair

via a secure wireless technology (e.g., Bluetooth, NFC, WiFi, etc.) or a wired connection, to exchange data. Once paired, a secure connection is established between both of the identity wallet applications on the owner's smart device and on the vehicle. Via his UI, the owner selects the specific VC he wants to transfer to his vehicle. After confirming his selection, the identity wallet application on the owners smart device prepares the selected VC for delegation by packaging the VC data and potentially adding metadata like expiration dates. With a cryptographic signature, the VC is then transmitted via the secury connection, to the vehicles identity wallet application. The "identity application" on the vehicle receives the signed VC and stores the it securely within the vehicle's internal storage. By making use of the smart vehicles UI, the vehicle owner can now configure his stored VC by setting up properties for selective disclosure of VC attributes or automataic presentation.

Verification Process

The verification process begins as soon as the smart infrastructure device detects the approaching smart vehicle with its wireless vehicle communication system, see Fig. 6.6. Once the vehicle is detected, the smart infrastructure initiates a wireless communication channel between itself and the vehicle. The smart infrastructure uses its verification agent to then generate an invitation for a secure one-time connection session. As the vehicles identity wallet application retrieves the verifiers invitation, it confirms the authenticity and trustworthiness of the infrastructure by looking up its identifier in the public list of trusted agents. If the device's authenticity cannot be verified, the vehicle might terminate the connection attempt to prevent an unauthorized or malicious connection. After verifying the smart infrastructure device's authenticity, the identity wallet application establishes the secure connection session.

Once the secure connection is established, the smart infrastructure device sends a ZKP request to the vehicles identity wallet application, which in return answers with the corresponding verifiable presentation, if available (see Fig. 6.7). The received verifiable presentation is then cryptographically verified by the credential verification agent using the public trust anchor and revocation tables. Based on the verification results, the smart infrastructures decision logic makes a decision regarding the vehicle's access or authorization. If the verification is successful, the device might grant the vehicle access to certain services or areas, if not other measures can be applied.

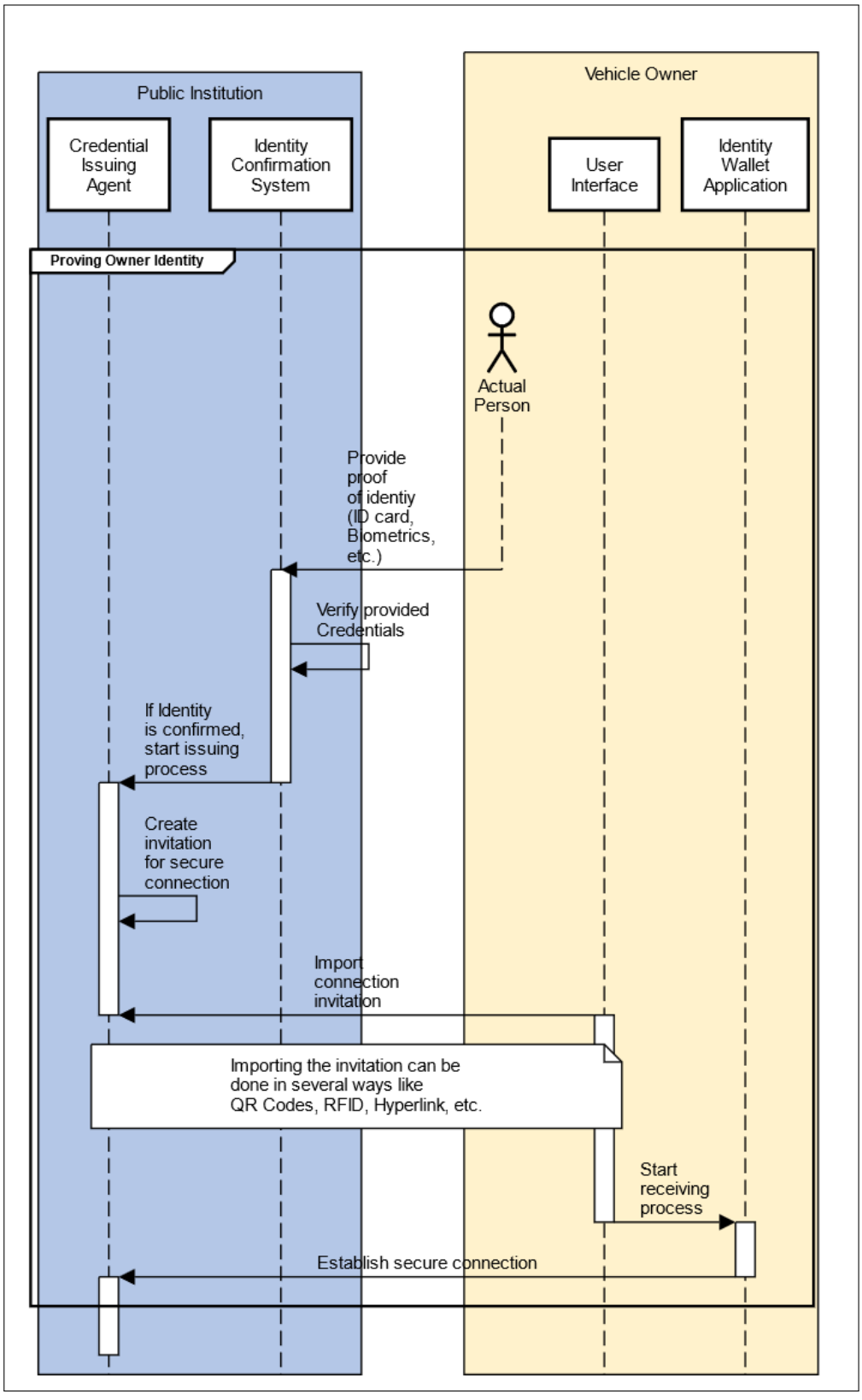

Figure 6.3: Sequence diagram of the connection establishing process between public institution and vehicle owner.

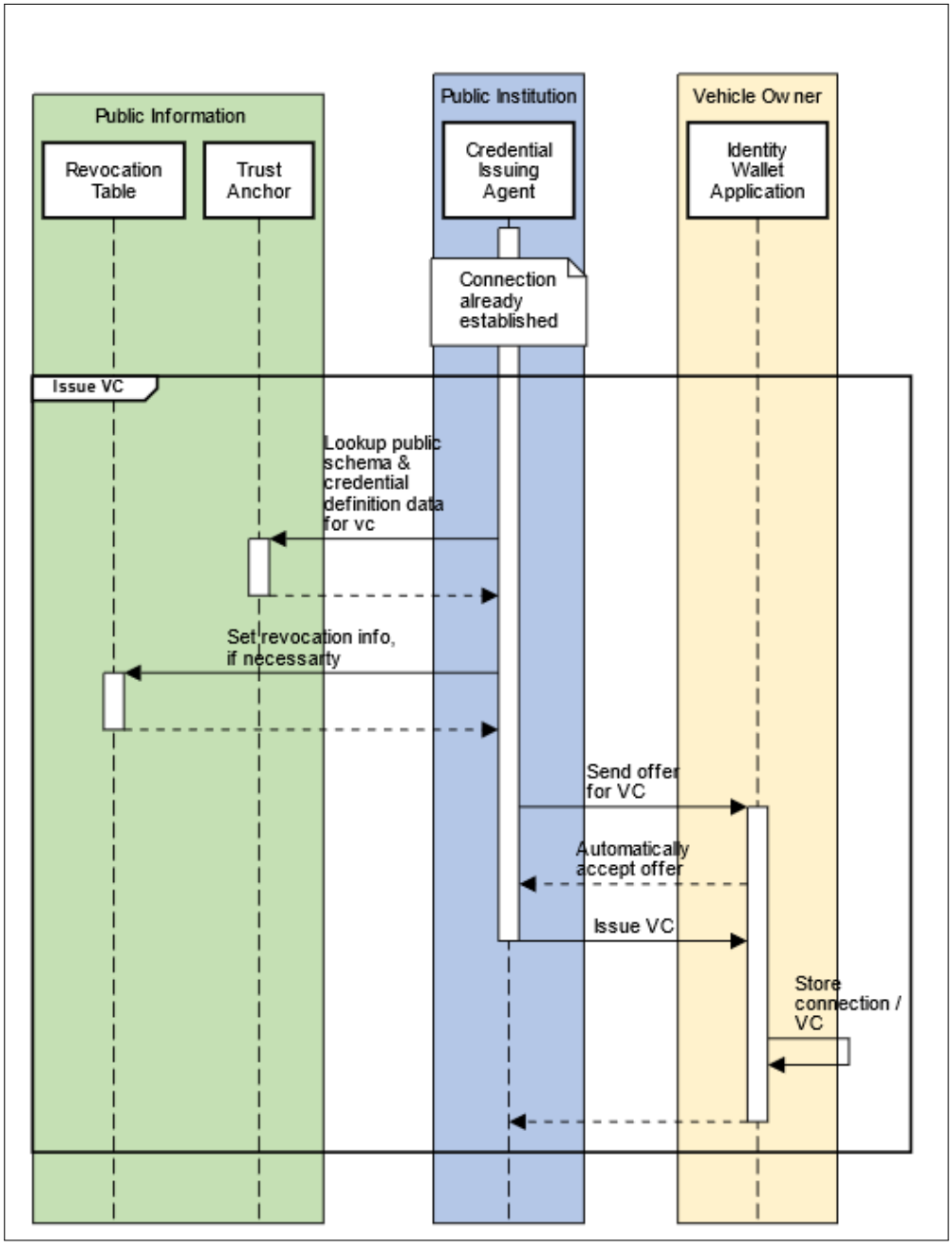

Figure 6.4: Sequence diagram of the issuing process between public institution and vehicle owner.

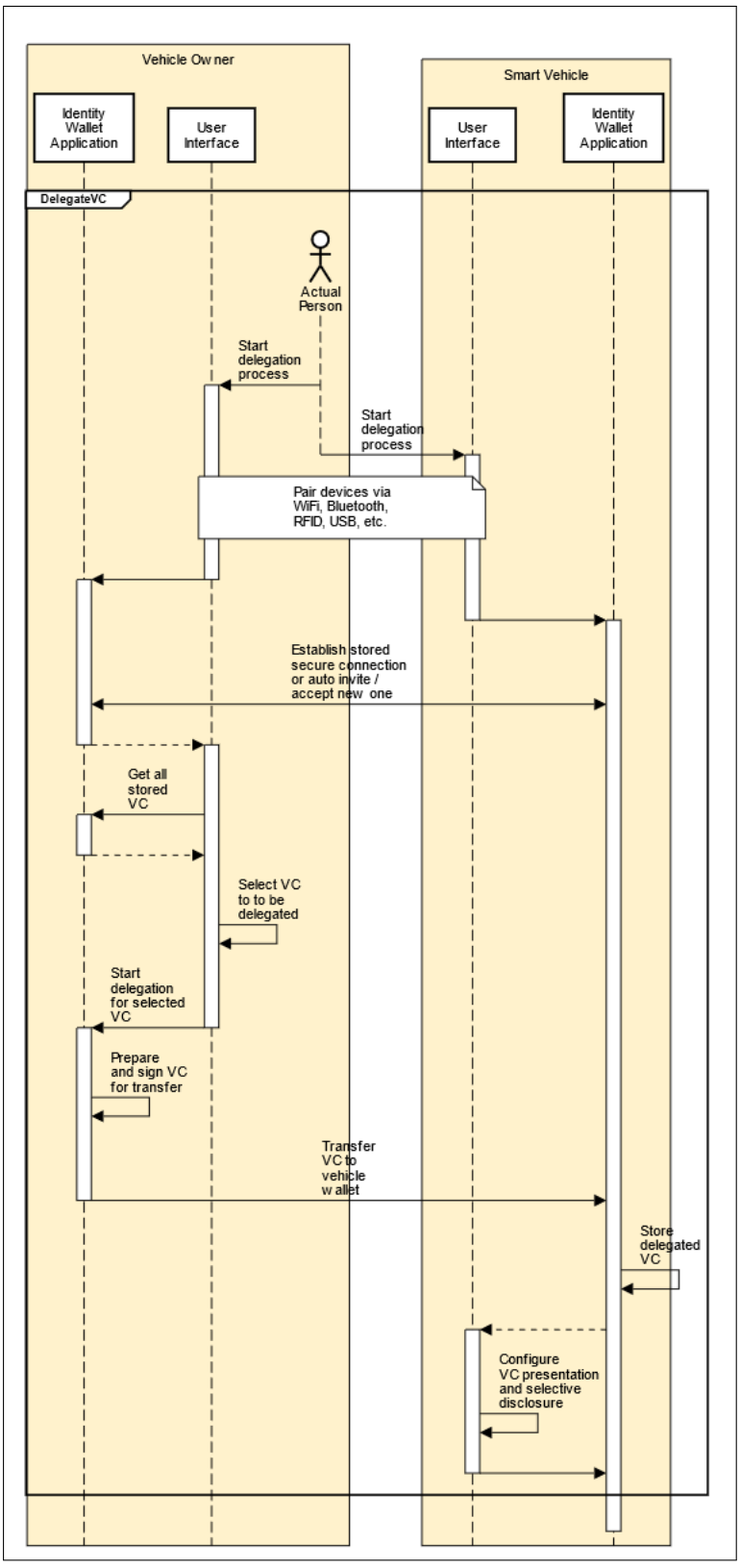

Figure 6.5: Sequence diagram of the delegation process between vehicle owner and smart vehicle.

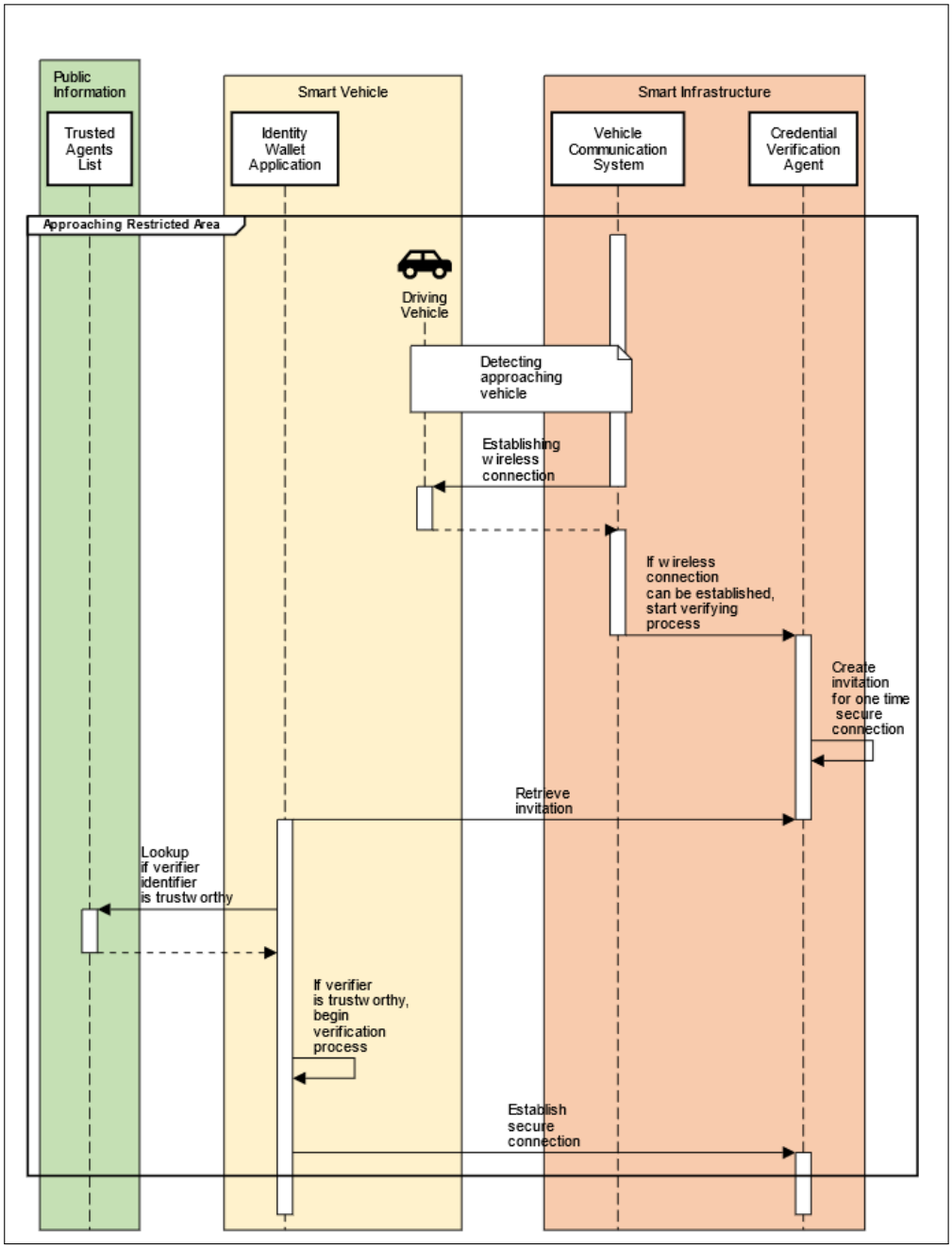

Figure 6.6: Sequence diagram of the connection establishing process between smart vehicle and infrastructure.

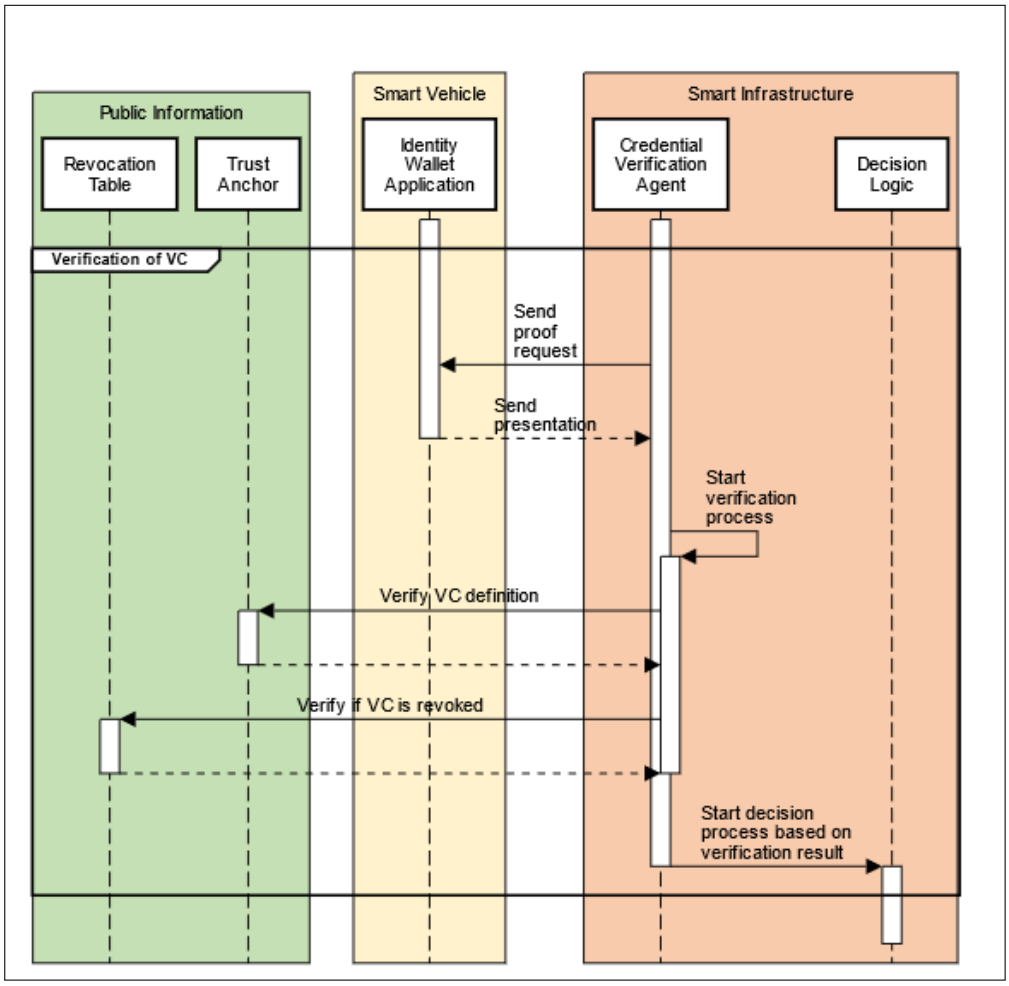

Figure 6.7: Sequence diagram of the verification process between smart vehicle and smart infrastructure.

7

EVALUATION PROCESS

Now that the architecture and functionality of the framework have been explained in chapter 6, I go into detail on how the evaluation process helps to achieve the final result. For this I explain the procedure of finding experts with a relevant background, conducting the interviews, coding of the qualitative data as well as drawing conclusions from the findings.

7.1 EVALUATION METHODOLOGY

Conducting expert interviews for evaluation purposes within the DSR methodology, involves a systematic approach to gather valuable insights from domain experts. The evaluation is done by experts in their respective fields, who have either practical experience, theoretical knowledge, or otherwise insights that provide valuable input to my research. After surveying the current landscape of researchers and engineers in the respective fields of decentralized identity, smart vehicles and IoT systems, I am able to identify and get in contact with several pundits whose area of expertise range from theoretical research over practical systems engineering to current European privacy laws and regulations. An overview of these experts, their area of expertise and the focus of the evaluation can be seen in Table 7.1.

The experts are contacted and asked to participate in the interview via email, professional networking platforms and in person due to previous encounters. When requesting the interview, I explain the purpose and process of my research, as well as the relevance of their expertise, and the potential impact of their contribution. I also emphasise the confidentiality of the experts names and their affiliation with any particular company, institute or publications.

Once the experts agree to participate, we schedule the interview. Conducting the interviews remotely have proven beneficial as they eliminate geographical limitations and allow for a broader pool of experts. I either use the software *Microsoft Teams* or *Zoom* under a GDPR compliant commercial or University licence for this, however some interviews are also done in person, when the schedule and proximity to the expert matches. During each interview, I follow the previously

#	Interviewed Expert (Alias)	Area of Expertise	Evaluation of DO	Evaluation of Arch.
Iteration Step I				
1.	Expert A	CIO of a company for decentralized identity solutions	X	X
2.	Expert B	Developer of IAM solutions and decentralized identity applications	X	X
3.	Expert C	Researcher of decentralized identity technologies	X	X
Iteration Step II				
4.	Expert D	Practicing Data Privacy lawyer	X	
5.	Expert E	Researcher of blockchain technologies	X	X
6.	Expert F	Researcher of decentralizing technologies and their regulation	X	X

Table 7.1: Interviewed experts for this thesis on each iteration step.

prepared interview guide (see Appendix A) with questions to the DO and present addition information on presentation slides, while I also follow unexpected lines of inquiry that emerge during the conversation to gain additional insights.

With the consent of the participants, I record all interviews for later transcription. For transcribing the whole conversation, I make use of the automated "Transcription" functionality of *Microsoft Word*, however manually corrections are still necessary to some passages of text. All transcripts can be read in Appendix C. The Transcription is crucial

as it allows me to have a textual record of the interviews to analyse the experts sentiment and assessment of DO, Framework architecture and Framework processes.

As textual data itself is hard to quantify, I make use of deductive coding system to identify and categorize the themes and patterns that occur in the conversations based on the codes (see Appendix B) [38]. By tagging appropriate text segments with the encoded categories, I can assign and assess the statements throughout all interviews. Once I applied the coding system to the interview data and categorized the insights provided by the experts, I extract the key findings from each interview.

I can now use the extracted key findings from the interviews to reiterate on the Framework architecture and processes as well as the DO. For this, I make sure to incorporate the relevant themes, suggestions, solutions, and insights into the design while at the same time improving identified weak points and errors. After the first iteration of conducted expert interviews, the now improved Framework is presented to experts in the second iteration, which results are again incorporated into the design.

Now with the evaluation methodology in mind, I go into detail on the actual insights I gained on the strengths and weaknesses of the Framework architecture and the understanding that follows. For this I focus on three core dimensions of the evaluation, the *Architecture and Component Evaluation* where I delve into an examination of the architectural processes and individual components, the *Design Objective Evaluation* where the degree to which the realized Framework aligns with the DO from chapter 5 is assessed, and the *Overall Feasibility Evaluation* that describes the overarching practical real-world feasibility.

7.2 ARCHITECTURE AND COMPONENT EVALUATION

Focusing the evaluation on the frameworks components introduced in chapter 6, allows me to systematically analyse the interactions, synergies, and potential friction points among these elements. The insights of the expert evaluation not only highlights the structural integrity and functional cohesiveness, but also identifies opportunities for optimization and refinement. By evaluating the interplay of components within the architecture, I gain valuable insights into the potential enhancements that can be incorporated in further iterations to elevate the overall architectural quality.

Public Institutions

The choice of using public institutions, as issuing entities within the framework are widely considered as conclusive useful by the experts during evaluation. Depending on the use case scenario, official entities like registration offices, health insurance companies, or driver's license offices, were discussed as well as private companies like toll collectors or parking lot providers. Expert D also mentions the currently discussed EU regulations for QTSP as issuers for Qualified Electronic Attestation of Attributes (QEAA), that would fit the role of a public issuing institutions, well. He also mentions, that it would be most likely an official requirement to have a strong legal backing of issued VC from public institutions, containing personal official data.

Vehicle Manufacturer

The consensus among the interviewed experts on the role of the vehicle manufacturer as an issuing entity, is somewhat less clear compared to that of the public institutions. This is mostly because of the ambiguity of the actual smart vehicle properties, that are issued and stored on the vehicles identity wallet application and their usefulness in real world scenarios. Designing a structured real world use case could help clarify the usefulness of issued vehicle VC from the manufacturer.

Vehicle Owner

As holder of the issued VC, the vehicle owner is a comprehensible choice for all experts as holding and managing his own VC is one of the core concepts of wallet-based identity management. The most discussed process was certainly that of the delegation of VC from the owner to the vehicle. Experts C, E, and F were most concerned of the practical feasibility of this process, as very little approaches of this have been implemented yet. However, other aspects like pairing up the owners smart device with his vehicle and using the controls of both UI are considered easily realizable.

Smart Vehicle

The smart vehicle with the two central responsibilities of holding its delegated VC and creating verifiable presentation out of them, is considered a key element within the framework. The experts C, E, and

F acknowledge the presented use cases for vehicles to pool different VC together, but think additional real world scenarios need to be found done to justify the implementations by institutions, manufacturers and private companies. Furthermore, more PoC of VC pooling IoT systems need to be implemented, according to expert C. Expert E also suggests an alternative to the delegation process, by forwarding incoming proof requests to the smart devices of its respective occupants, to be answered there directly.

Smart City Infrastructure

Utilizing smart city infrastructure as verifiers was met with a lot of technical concerns by the experts. The wireless communication between one or more, potentially fast, moving vehicle and a infrastructural IoT device poses challenges depending on the protocol and transmission hardware, remarks epxert A. Expert C doubts the practical equippability and upgradeability of existing infrastructure such as street lamps and traffic lights, as well as the physical security of additional hardware modules in easy accessible places. He is also concerned about the creation of movement profiles created by statistical correlation from a tight mesh of infrastructure devices within a city, recording vehicles.

Public Available Information

Summarizing the the trust anchor, revocation table and trusted agent list within a public available information entity is met with agreement among the experts. Though the exact implementation of the trust anchor - whether a DLT, Public Key Infrastructure (PKI) based certificates or other technology is used or not - is up for debate, the necessity of publicly accessible schemas, definitions, cryptographic public keys, etc. seems clear and is emphasised by expert B, C and E. While the revocation of issued VC for the vehicle owner is already, well covered by the established wallet-based identity concepts, the revocation or expiration of delegated VC is still under development, remarks expert E.

Vehicle passengers

Adding potential passengers to extend the framework architecture is considered novel by the experts in the context of multiple different entities delegating their VC to a common pool (i.e. the smart vehicle).

Despite this new conception, the experts consider it possible in principle.

7.3 DESIGN OBJECTIVE EVALUATION

Now that the components of the framework are evaluated individually, I rigorously assess if the realized design aligns with the five predefined DO and their respective requirements introduced in chapter 5. This expert evaluation provides a comprehensive perspective on the efficacy of the designed framework in meeting the intended goals.

Objective 1: Reliable management of identities and credentials

Its core mission of providing a reliable identity management for its users is fulfilled by the wallet-based framework, by utilizing user wallets, unique identifiers, and VC to provide ways of verification. While the handling of individual wallets and VC is done by each individual holder, issuers and verifiers still rely on a centralized authority to be managed.

Requirements:

1. **Ensuring trust between Participants**:
   Trust is ensured by a publicly available data trust anchor and strong cryptographic processes for all transferred data between all participants.

2. **Decentralization**:
   As the creation and management of identity wallets can be handled completely without any central authority, their usage can be considered sufficiently decentralized. However, as official public institutions and public infrastructure remain centrally governed by the respective authority, a completely decentralized framework is not possible this way.

3. **Unique identifiers**:
   Creating and managing unique identifiers to communicate within the framework is a core functionality of every identity wallet application, issuing agent and verification agent.

4. **Processing of verifiable attributes**:
   The use of VC that attest its holder certain attributes, not only allows the efficient and reliable issuance of such, but additionally provides ways to easily and reliably verify their authenticity, revoke them after expiration, and delegate them to another wallet.

Objective 2: System security

The framework provides an elaborate approach on system security, where the integrity, confidentiality and availability of its participants is ensured by the incorporation of widely approved security concepts. Potentially compromising threats are encountered with extensive use encryption, robust transmission and strong authentication schemes.

Requirements:

1. **Encrypted data storage and transfer**:
   The use of cryptographic methods within the identity Wallet application of the vehicle and its owner, as well as in the secure communication processes, fulfills this requirement. Yet, depending on the jurisdiction these methods need to be compliant with official regulations and governmental recommendations to be used by public institutions (as the case is in Germany [13]).

2. **Robust transmissions**:
   Using tried and tested methods for reliable wireless or wired data transfer between all framework entities ensures the availability of each established connection. Secure one-time communication channels hamper attempts to Man-in-the-Middle (MITM) or Replay attacks [2, 20].

3. **Authentication of issuers, holders, and verifiers**:
   Due to the presentation of a reliable identity proof of the holder during the issuing process, the authenticity of a holder can be ensured. Using a publicly available list of trusted agents to look up the unique identifier of a issuer or verifying device, also helps authenticate trustworthy institutions and verifiers.

4. **Tamper proof identifiers**
   Embedding unique identifiers into, sometimes several, hardware components of vehicles or into cryptographically secure storage modules within a smart device of a vehicle owner, increases security and hampers malicious spoofing attempts.

Objective 3: Privacy protection and legal compliance

While the approaches that are made by the framework to ensure user privacy and data minimization, the legal and regulatory environment is not yet comprehensively available enough, to ensure compliance. However, as these regulations are currently being worked on, this

may change in future.

Requirements:

1. **Legal Compliance**:
   Fulfilling legal compliance is difficult, as it is highly dependent on the jurisdiction in question. In the EU, a lot of regulatory effort is currently being made to establish wallet-based identity technology [12], but as the topic of wallet-based identity management is still quite new regarding regulations, its establishment and that of technologies like VC or ZKP may be a ongoing changing topic for the foreseeable future.

2. **User- and Meta-Data Minimization**:
   The utilization of ZKP for the verification process in the framework, allows a data minimizing way to ensure the identity of owner or vehicle VC without revealing any sensitive information during transmission [33].

3. **Explicit User Consent and selective disclosure of information**:
   With the ability to control and configure die holders VC with his own UI as well as the UI of his vehicle gives him the ability to precisely set how his VC are stored and what attributes are shared. This is very important as the automatically answering to proof requests from any verifier would otherwise potentially leak information to unwanted entities.

Objective 4: Interoperability between systems, authorities and users

The open and interoperable nature of the framework holds much potential for a widely spread extensible ecosystems, where issuing entities, vehicles and VC holders can easily join. However, a big effort in standardizing key aspects of the delegation and verifying processes, still has to be made to enable this adoption. Overcoming this challenge requires the right incentives to the potential participants to come to an agreement on these standards.

Requirements:

1. **Standardized communication protocols and data formats**:
   Using already existing transfer protocols for the physical connections between all entities greatly improved standardization, while orienting on currently defined standards like World Wide Web Consortium (W3C) for DID and VC, ensures further adoption.

As technologies for ZKP and Authentic Chained Data Containers (ACDC) also become more and more prevalent, further steps for a completely standardized ecosystem are made.

2. **Nonexclusive system support**:
   The framework is designed and evaluated with no specific system in mind. Every component and every process functionality is possible without utilizing vendor specific hard- or software.

Objective 5: Effective usability

The usability of the framework highly depends on its ability to keep its complexity at a minimum, while at the same time efficiently scale up with an increasing number of participants and users. Even as the framework architecture itself is kept comparably simple, the challenges that come with working on IoT devices and smart vehicles remain hurdles to be overcome.

Requirements:

1. **Minimal complexity**:
   Minimizing complexity is difficult in any sufficiently large distributed system. While the framework itself can described with only using six, respective seven, different kinds of participants, the need for cryptographic PKI for a large amount of infrastructural devices, the large amount of communication necessary within the processes and the potentially complex sub-components on their own, all increase overall complexity of the framework.

2. **Efficient scaling**:
   Due the open and decentralized nature of the wallet-based concept, the scaling of issuing and holding entities is considered quite good []. At the same time, physical constrains of the wireless connections between vehicle and infrastructure remain as a bottleneck for increasing the number of vehicles per verifying device.

3. **Intuitive user interfaces**:
   That every user has a sufficient and user-friendly interface to interact with the framework, is ensured through the UI subcomponents of each holding entity as well as well as the *Identity Confirmation System* of the public institution.

7.4 OVERALL FEASIBILITY EVALUATION

After these extensive expert evaluations of the frameworks components, processes and fulfilled DO, the question of the actual real world feasibility remains open. The frameworks architecture and information flow have largely garnered approval by the interviewed experts and the resemblance to already existing wallet-based identity scenarios was recognized. All experts were basically in agreement, that the challenges of vehicle identification can be met with a wallet-based approach. While experts A, B, D and F mostly see the frameworks potential in its usage for identifying access to restricted city areas, expert C and E see the advantages in a more monetizable use cases such as paying for parking lots. Expert E additionally remarks positively the paradigm shift from being passively recorded as a vehicle to initiating the verification process.

All interviewed experts also identified certain limitations that warrant consideration for an actual application. The lack of existing software implementations regarding wallet-based identity management is pointed out by experts A and C. Especially widely used and reliable software libraries for comprehensive delegation of the issued VC or ZKP support, are needed to realize this framework to full extent. The political will and ability to establish the framework is doubted by experts A, D and E. Either because the possibility to use the gathered data for surveillance purposes is seen as a "desired side effect" (Expert A), the governmental institutions have a direct "interest in increasing surveillance" (Expert D) or because it would "be too hard to convey the abstract concepts like SSI or ZKP" (Expert E). Another point to be considered was brought by expert B, when discussing the accessibility of the frameworks technology and processes for people who require analogue alternatives and may not be excluded from official services. Alternative processes for these people may be required for issuing or verification.

Implementing the smart city infrastructure is seen as a weak spot by Expert C, as he criticises the high complexity of a widely spread PKI necessary to give each infrastructure device a sub component for V2X communication, especially considering the long lasting development and maintenance cycles. Additionally, experts A and C have raised concerns about the scalability of the proposed framework when the number of smart vehicles and their connection requests within cities increase. Issues related to latency and responsiveness in high-traffic scenarios need to be thoroughly addressed to prevent disruptions in real-time communication between vehicles and infrastructure. Expert

C also warns of the potential danger of deanonymizing users by using statistical correlation of their attributes and meta data gathered from the vehicle when establishing connections.

8

DISCUSSION

With the theoretical background from chapter 2 and the definition of the framework in chapter 6, I am now able to discuss the results of the evaluation process from chapter 7 from different perspectives. For this I summarize the key findings regarding the research question, of whether a wallet-based identity framework can improve smart vehicle identification, and also subsequently list the potential benefits as well as remaining challenges of said framework.

8.1 KEY FINDINGS

The extensive research in the fields of IoT, wallet-based identity and smart vehicles during the development of my framework, as well as the insights from the expert evaluation, yielded four important findings that there are *Improvements for vehicle identification*, the *Necessity for technological standardization*, the *Necessity for legal frameworks*, and lastly an existing *Implementation Gap*. These findings, as seen in table 8.1, help to further highlight the relevant results of this thesis and its possible impact for future research.

1. Improvements for vehicle identification

Presenting the potential substantial benefits for improving smart vehicle identification of the framework to the experts is generally received by approval. Through the utilization the combined properties of IoT based smart vehicles and wallet-based identity management, a secure, accurate, extensible and privacy conserving alternative to prevalent vehicle monitoring approaches can be achieved.

2. Necessity for technological standardization

The interviews revealed that the lack of uniform communication protocols across various smart vehicle systems and wallet-based identity frameworks. This poses significant challenges to seamless interaction and data exchange and stresses the importance of developing standardized protocols and implement PoC that enable interoperability,

3. Necessity of legal certainty

The expert interviews consistently highlight the imperative need for establishing robust legal frameworks and regulations (e.g. eIDAS) to accompany the deployment of the framework. Clear and comprehensive guidelines are crucial to address concerns pertaining to data privacy, liability, and ownership. Achieving this, may be accelerated by increasing public understanding and raising political awareness about the benefits of those frameworks.

4. Implementation Gap

As already mentioned by numerous experts during the conducted interviews, the current lack of widespread implementations prevents a more detailed assessment of their feasibility in real world scenarios. This relates to key aspects of the framework such as delegation or ZKP processes, the development of IoT system for physical V2X connection, as well as the implementations of wallet-based identity frameworks in general.

#	**Finding**	**Description**
1.	Improvements for vehicle identification	The framework shows potential for improving vehicle identification in smart cities.
2.	Necessity for technological standardization	The lack of standardized practices hinders interoperability and scalability for real world implementations.
3.	Necessity of legal certainty	The importance of establishing and widely adopting legal frameworks and regulations for the implementation of any the wallet-based identity systems becomes apparent.
4.	Implementation Gap	More implementations of relevant technologies are necessary to assess and improve their feasibility in real world scenarios.

Table 8.1: Summary of key findings of the framework evaluation.

8.2 BENEFITS AND CHALLENGES

Besides the aforementioned key findings, the expert evaluation of the framework also reveals several benefits of its usage as well as challenges to overcome when deploying the framework. In table 8.2 I summarize the four most outstanding benefits as well as the three most pressing challenges.

Benefit: Direct vehicle communication

One of the biggest benefits is the frameworks shift from current camera based systems, monitoring a whole street segment at all time and thus even every uninvolved traffic participant, to a direct V2X approach. Now, a identification process is only directly established and perfomed between the vehicle and the infrastructure itself. No uninvolved bystanders are affected by this system, which improves overall privacy of all city residents. A direct V2X communication additionally increases identification accuracy, as the wireless connection is less subject to environmental conditions such as OCR within ANPR systems [24] and rules out false positives/negatives.

Benefit: Data minimization and increased privacy

Once the connection is established, another benefit comes to play: the data minimal conception and the utilization of ZKP allow for a verification of VC without revealing sensitive information about its holder. This greatly increases privacy for the vehicle owner and driver, as no lookup into any central registry is necessary.

Benefit: Easy extension of ecosystem

Another benefit is the possibility to hold and manage the VC from multiple public issuers and even issued vehicle properties to use them for verification for their respective use. The interoperable nature of wallet-based ecosystems allows easy adoption for new service providers that have a monetary incentive, but value data minimizing systems. With an increasing number of issuers, verifiers and attached services, the value of this systems also increases for the vehicle owners and passengers.

Benefit: Delegation and pooling of permissions/credentials

The holder of VC is also able to delegate his credentials to any vehicle he has access to and even pooling several VC from multiple vehicle occupants, to share their permissions with each other, is possible by using wallet-based identity frameworks. This offers new possibilities in how people interact with their vehicles, by encouraging car sharing and car pooling concepts.

However, there are of course challenges to solve, should the framework be deployed for real world applications.

Challenge: Complex and costly implementation / operation

Implementing and operating a distributed system of the scale of a city district with multiple interconnected wallet applications, issuing and verification agents and the PKI to allow them to be cryptographically verifiable, is a very sophisticated and complex project that involves a lot of planning and maintenance to be successful, as also remarked by expert C. Increased complexity is also associated with higher costs for the operator compared to the cheap, already established systems [30].

Challenge: Inteaction with competing systems, standards and regulations

Already established systems as well as competing standards and protocols pose a challenge to the framework as compatibility and interoperability highly rely on using the same implemented technologies. Creating possibilities to connect with systems and technologies outside the predefined ecosystem, may be crucial for the successful deployment in real world scenarios.

Challenge: Political / sociatal acceptance necessary

However, one should also not underestimate the political and societal component that comes with driving novel technologies forward, especially when they are as deeply embedded into peoples daily lives as identity management. For people to actually install a wallet identity application onto their smart vehicles and devices, and for cities switch from the established forms of traffic monitoring, a wide acceptance of the technology must be there. This acceptance requires a basic understanding of the theoretical foundations wallet-based iden-

tity management is build upon and can be hard to convey. Lastly, a political will of city officials, to decide against surveilling camera systems, is necessary.

Benefits	**Challenges**
Direct vehicle communication	Complex and costly implementation / operation
Data minimization and increased privacy	Interaction with competing systems, standards and regulations
Easy extension of ecosystem	Political / societal acceptance necessary
Delegation and pooling of permissions/credentials	

Table 8.2: Comparison of the frameworks benefits and challenges.

9

CONCLUSION

This final chapter serves as a conclusion and outlook into potential future work based on the findings of this thesis. I draw my conclusion of the research question from chapter 1 and describe how future research can build upon on it. For this, I first summarize my research approach and methodology in this work followed by open challenges that need to be resolved in future.

To answer the research question of whether a wallet-based IoT identity framework for smart vehicles can actually improve vehicle identification in smart cities, I researched and assessed existing vehicle identification systems. After analysing the necessary requirements, I followed the DSR approach by deriving five DO and developing a framework architecture along with its internal processes as an artefact. To refine this artefact I iterated through two rounds conducting expert interviews for evaluation and incorporating the resulting insights. After discussing the key findings and conclusions they can now be found in this thesis in order to serve as a documentation and starting point for future research in this or a related area. While it lies in the iterative nature of DSR that artefacts like this framework architecture and its processes can always be improved and refined, I can already say that using wallet-based identity management in the context of smart cities and vehicles, serves as an excellent use case to drive the research and technological development even further. The insights found from the conducted expert interviews done for this thesis, confirm me in my believe that this approach in vehicle identification with its benefits shows much potential to serve as an alternative to the common passive monitoring systems prevalent in urban landscapes.

The mentioned challenges, that became apparent through the rigorous expert evaluation, however indicate the long and effortful way that still lies ahead of the researchers in this field, to make this or similar frameworks a reality. Working on widely accepted standards and protocols, establishing the legal and regulatory basis, raising political awareness, planning city-wide infrastructure, or developing new systems to implement PoC are no easy tasks and will probably not be completed within a short couple of years. Establishing novel identity management technology however, may be worth the effort.

A

APPLIED INTERVIEW GUIDES

Interview guide to serve as a loose memory aid during the expert interviews.

ENGLISH

1. Introduction
    - Welcome / Introduction
    - Clarification of interview language
    - Introduction of the topic
    - Clarification of interview procedure / duration
    - Privacy agreement / note on confidentiality
2. Opening questions
    - What is your research topic / area of expertise?
    - How long have you been working in the field?
    - Are you familiar with the term (decentralized) identity management?
    - Where in your field have you had contact points with the management of different identities?
3. Evaluation
    a) Subject: Decentralized identities
        - How do you evaluate the development of decentralized (self-sovereign) identity technologies?
            - What are the advantages and disadvantages compared to "classic" centralized identity technologies?
        - In your opinion, should SSI be used / promoted by public institutions (as issuers and verifiers)?
            - What should be considered when public institutions act as exhibitors or verifiers in the SSI context?
        - Should smart (IoT) devices or vehicles play a role in SSI?
            - For what purposes is this appropriate?

  - What are the advantages/disadvantages of this?
  - How do you evaluate the transfer of VC to smart devices?

b) Field: IoT / Smart Vehicles
   i. How do you see the development of smart cars?
   ii. How do you evaluate the current (centralized) fomen of identification of vehicles? (ANPR, IMSI, GPS tracking, transmission of chassis numbers).
      - What are the most common forms currently?
      - How do you estimate the future?
      - Do you see a need for decentralized solutions?
   iii. How do you evaluate digital identity wallets in vehicles and public infrastructure?
      - What vehicle properties do you think would be interesting to store in such a wallet?
      - Are the storage technologies for encrypted wallets available?
      - What are the biggest challenges to overcome?
      - Which facilities are best suited (traffic lights, lanterns, signs, etc.)?
      - What transmission media / protocols are best suited here?
      - What are the technical limitations here?
   iv. How do you rate the communication between occupants and vehicle?
      - Which technology is better for this (NFC, Bluetooth, WiFi, [cable?], etc.)?
      - What are the technical limitations here?

c) Subject: Smart City
   i. How do you see the development of smart cities?
      - What do you think are the three main characteristics of a Smart City?
      - What are the main advantages and disadvantages to the concept?
   ii. Do you think the need for access restrictions (due to resident, environmental, or other reasons) will increase in the future?

- How should access restrictions be managed/monitored to that end?

iii. How do you see that the issue of centralized monitoring of people/vehicles in smart cities?
- Is there a need for decentralized solutions like on the chart?
- What goals do you think are still missing?

iv. How do you see the need for smart vehicles?
- How do you see the need for vehicle-to-infrastructure communications? (As shown in the diagram?)
- Which urban infrastructure do you think is best suited for vehicles to communicate? (Lanterns, traffic lights, signs, bollards, etc.).

v. What is your opinion about individual transport in cities/metropolitan areas?
- Where is the number of individual vehicles going / where should it go? / Why?

d) How do you evaluate the design objectives of the framework?
- Reliable identity management
- System security ensured
- Data protection ensured
- Interoperability possible
- Efficient usability
- What objectives do you think are still missing?

e) Framework architecture

i. How do you evaluate the architecture of the framework in the simple case (institution - driver - vehicle - infrastructure)?
- Basic structure of the approach
- Weaknesses of the approach

ii. How do you evaluate the process flow in general?
- Basic structure of the decentralized approach

iii. Fulfillment of the design objectives

A. Can identities be reliably managed and credentials issued using this framework?

B. Is system security guaranteed?

C. Is data protection guaranteed?

D. Is there a possibility for interoperability?

E. Can the architecture be used efficiently?

iv. What would argue against the implementation of the architecture?

- What factors / stakeholders would oppose it?

4. Summary

a) Do you have any questions or further thoughts about this topic or the interview itself?

b) Summary of the interview

c) Can you think of any other potential interviewees?

5. Conclusion

a) Upon request: sending the summary of the framework.

b) Farewell

GERMAN

1. Einführung
   - Begrüßung / Vorstellung
   - Klärung der Interviewsprache
   - Vorstellung des Themas
   - Klärung von Ablauf / Dauer des Interviews
   - Datenschutzvereinbarung / Hinweis auf Verschwiegenheit
2. Eröffnungsfragen
   - Was ist Ihr Forschungsthema /-Fachgebiet?
   - Wie lange arbeiten Sie schon in dem Bereich?
   - Kennen Sie den Begriff (dezentrales) Identitätsmanagement?
   - Wo haben Sie in Ihrem Fachgebiet schon einmal Berührungspunkte mit der Verwaltung verschiedener Identitäten gehabt?
3. Evaluation
   a) Fachgebiet: Dezentrale Identitäten
      - Wie bewerten Sie die Entwicklung der dezentralen (self-sovereign) Identity technologien?
        – Was sind die Vor- und Nachteile gegenüber "klassischen" zentralisierten Identitätstechnologien?
      - Sollte Ihrer Meinung nach SSI von öffentlichen Institutionen genutzt / gefördert werden (als Aussteller und Überprüfer)?
        – Was ist zu beachten wenn öffentliche Institutionen als Aussteller oder Überprüfer im SSI-Kontext auftreten?
      - Sollten Smarte (IoT) Geräte oder Fahrzeuge in SSI eine Rolle spielen?
        – Für welche Einsatzzwecke ist dies geeignet?
        – Welche Vor-/Nachteile ergeben sich daraus?
        – Wie bewerten Sie die Übertragung von VC auf Smarte Geräte?

   b) Fachgebiet: IoT / Smart Vehicles
      i. Wie sehen sie den Entwicklung von Smart Cars?
      ii. Wie bewerten Sie die aktuellen (zentralisierten) Fomen von Identifikation von Fahrzeugen? (ANPR, IMSI, GPS tracking, übermittlung von Fahrgestellnr.)

- Welches sind die gängisten Formen aktuell?
- Wie schätzen Sie die Zukunft dahingegen ein?
- Sehen Sie einen Bedarf für dezentrale Lösungen?

iii. Wie bewerten Sie digitale Identity-Wallets in Fahrzeugen und öffentlicher Infrastruktur?

- Welche Fahrzeugeigenschaften wäre Ihrer Meinung nach interessant in einem so Wallet zu speichern?
- Sind die Speichertechnologien für verschlüsselte Wallets vorhanden?
- Was sind die größten Herausforderungen, die es zu bewältigen gillt?
- Welche Anlagen eignen sich am besten (Ampeln, Laternen, Schilder, etc.)?
- Welche Übertragungsmedien / -protokolle sind hier am besten geeignet?
- Welche technischen Limitierungen gelten hier?

iv. Wie bewerten Sie die Kommunikation zwischen Insassen und Fahrzeug?

- Welche Technologie ist hierfür besser geeignet (NFC, Bluetooth, WiFi, [Kabel?], etc.)?
- Welche technischen Limitierungen gelten hier?

c) Fachgebiet: Smart City

i. Wie sehen Sie die Entwicklung von Smart Cities?

- Was sind Ihrer Meinung nach die drei Hauptmerkmale einer Smarten Stadt?
- Was sind die Hauptvor- und nachteile an dem Konzept?

ii. Denken Sie, dass der Bedarf an Zugangsbeschränkungen (aufgrund von Anwohner-, Umwelt- oder sonstiger Gründe) in Zukunft zunehmen wird?

- Wie sollten Zugangsbeschränkungen dahingehend verwaltet/überwacht werden?

iii. Wie sehen Sie, dass das Thema zentraler Überwachung von Personen/Fahrzeugen in smarten Städten?

- Gibt es Bedarf an dezentralen Lösungen wie auf dem Schaubild?
- Welche Ziele fehlen Ihrer Meinung nach noch?

iv. Wie sehen Sie den Bedarf an Smarten Fahrzeugen?
   - Wie sehen Sie den Bedarf an Fahrzeug-zu-Infrastruktur-Kommunikation? (Wie im Schaubild gezeigt?)
   - Welche städtische Infrastruktur eignet sich Ihrer Meinung nach am besten um Fahrzeugen zu kommunizieren? (Laternen, Ampeln, Schilder, Poller, etc.)

v. Was ist Ihrer Meinung zum individualverkehr in den Städten/Ballungszentren?
   - Wohin Entwickelt sich die Zahl der individuellen Fahrzeuge / wohin sollte sie sich Entwickeln? / Warum?

d) Wie bewerten Sie die Design Objectives des Frameworks?
   - Zuverlässig Identitätsmanagement
   - Systemsicherheit gewährleistet
   - Datenschutz gewährleistet
   - Interoperabilität möglich
   - Effiziente Nutzbarkeit
   - Welche Ziele fehlen Ihrer Meinung nach noch?

e) Frameworkarchitektur

i. Wie bewerten Sie die Architektur des Frameworks im einfachen Fall (Institution - Fahrer - Fahrzeug - Infrastruktur)?
   - Grundaufbau des Ansatzes
   - Schwachstellen des Ansatzes

ii. Wie bewerten Sie den Prozessablauf grundsätzlich?
   - Grundaufbau des dezentralen Ansatz

iii. Erfüllen der Design Objectives

   A. Lassen sich mit diesem Framework zuverlässig Identitäten verwalten und Credentials ausstellen?
   B. Ist die Systemsicherheit gewährleistet?
   C. Ist der Datenschutz gewährleistet?
   D. Besteht die Möglichkeit zur Interoperabilität?
   E. Ist die Architektur so effizient nutzbar?

iv. Was würde gegen die Umsetzung der Architektur sprechen?
   - Welche Faktoren / Akteure würden sich dagegen aussprechen?

4. Zusammenfassung
    a) Haben Sie noch Fragen oder weitere Gedanken zu diesem Thema oder dem Interview selbst?
    b) Zusammenfassung des Interviews
    c) Fallen Ihnen noch weitere potentielle Interviewpartner ein?
5. Schluss
    a) Auf Wunsch: Zusendung der Zusammenfassung des Frameworks
    b) Verabschiedung

B

CODING SYSTEMS

Coding Categories
1. Design Objectives
1.1. Reliable management of identities and credentials
1.1.1. Feasibility
1.1.2. Usefullness
1.2. System security
1.2.1. Feasibility
1.2.2. Usefullness
1.3. Privacy protection and legal compliance
1.3.1. Feasibility
1.3.2. Usefullness
1.4. Interoperability between systems, authorities and Users
1.4.1. Feasibility
1.4.2. Usefullness
1.5. Effective usability
1.5.1. Feasibility
1.5.2. Usefullness
2. Framework Components
2.1. Architecture
2.1.1. Base Case
2.1.1.1. Public Institution (Issuer)
2.1.1.1.1 Problems
2.1.1.1.2.Consensus
2.1.1.2. Manufacturer (Issuer)
2.1.1.2.1. Problems
2.1.1.2.2. Consensus
2.1.1.3. Vehicle Owner (Holder)
2.1.1.3.1. Problems
2.1.1.3.2. Consensus
2.1.1.4. Vehicle (Holder)
2.1.1.4.1. Problems
2.1.1.4.2. Consensus
2.1.1.5. Infrastructure in Smart City (Verifier)
2.1.1.5.1. Problems
2.1.1.5.2. Consensus
2.1.1.6. Publicly Available Information
2.1.1.6.1. Problems

2.1.1.6.2. Consensus
2.1.2. Extended Case
2.1.2.1. Passenger (Holder)
2.1.2.1.1. Problems
2.1.2.1.2. Consensus
2.2. Processes
2.2.1. Base Case
2.2.1.1. Issuing to Vehicle Owner
2.2.1.1.1. Problems
2.2.1.1.2. Consensus
2.2.1.2. Delegation to Vehicle
2.2.1.2.1. Problems
2.2.1.2.2. Consensus
2.2.1.3. Issuing to Vehicle
2.2.1.3.1. Problems
2.2.1.3.2. Consensus
2.2.1.4. Presenting Proof to Infrastructure
2.2.1.4.1. Problems
2.2.1.4.2. Consensus
2.2.1.5. Public Information lookup
2.2.1.5.1. Problems
2.2.1.5.2. Consensus
2.2.2. Extended Case
2.2.2.1. Issuing to Passenger
2.2.2.1.1. Problems
2.2.2.1.2. Consensus
2.2.2.2. Delegation to Vehicle
2.2.2.2.1. Problems
2.2.2.2.2. Consensus
3. Overall Feasibility
3.1. Problems
3.2. Consensus

C

INTERVIEW TRANSCRIPTS

Abbrevations:

- **H:** - Interviewer,
- **A:**/**B:**/C:/**...** - Interviewed Expert

TRANSCRIPT: EXPERT A (GERMAN)

H: [...] Mich kennst du ja schon einmal für dich. Wie lange bist du denn bereits im Thema SSI aktiv?
A: Seit 2015.
H: 2015, ja.
A: Also schon 8 Jahre.
H: Hast du irgendwelche bestimmte Schwerpunkte oder hast du da in irgendeiner Art und Weise ein bestimmtes Steckenpferd?
A: Naja, grundsätzlich ist ja das ganze Thema SSI erstmal nicht nur eine technische Sache, sondern ein Paradigma. Und das ist ja aufgekommen als so dieser ganze Blockchain-Hype war und ganz oft wird es da in einen Topf geworfen, was ungerechtfertigt ist. Und wir haben uns halt oder ich auch. Insbesondere haben uns von Anfang an damit beschäftigt, was hat das für Implikationen auf bestehende Systeme in Unternehmen, vor allen Dingen im Bereich Identity und Access Management, weil da habe ich auch viele Projekte vorher schon gemacht und hab halt geguckt, wie kann man mit Verifiable Credentials und das was Leute in der Wallet haben, die Bereiche rund um Identity und Access Management, also sprich Entscheidungen für Berechtigungen – ja / Nein - befüllen und das, das ist so mein Steckenpferd, das hat sich über die Jahre dann aber daraus hinaus darüber hinaus entwickelt. Wie kann man Geschäftsprozesse die in Unternehmen oder jede beliebige Organisation heute abbildet, mit Verifiable Credentials oder Daten aus dem Credentials anreichern oder die auch in Gödens ausstellen, das heißt also, wie kann man eigentlich bestehende Geschäftsprozesse oder nicht-digitale Geschäftsprozesse auch gerne abbilden mit Verifiable Credentials.
H: Also ich gehe mal davon aus, wenn ich dich Frage, wie du das das Thema Self Sovereign Identity bewerten würdest, wärst du da eher zugeneigt und bist ein Befürworter dafür.
A: Ja, natürlich sehr. Dezentrale Identität ist was, was bisher nicht

genügend betrachtet wurde, wo viele inklusive mir, nicht glücklich sind, ist der Begriff Self Service Identity. Da haben wir einen. Komisches Fahrwasser gekommen, was eben dieses selbst Souveränität betrifft, also von wegen das klingt so ein bisschen also lehnt man Staat oder irgendwie verschiedene staatliche Institutionen ab, und das ist im Gegenteil eigentlich der Fall, das heißt, man will ja einen regulierten Rahmen Schaffen für genau diese dezentralen Mechanismen und Bürgerinnen und Bürger stärken in ihrer Entscheidungsfähigkeit, was Datenschützer betrifft. Das heißt, der Begriff ist misleading, aber das Konstrukt an sich und die Idee, man stellt die den Menschen in den Mittelpunkt, für die Datenflüsse, das finde ich super. Und ich glaube, dass ich mehr oder weniger der Begriff dezentrale Identität einbürgert und das wahrscheinlich der Begriff Self-Sovereign Identity ein bisschen in den Hintergrund gelangen wird.
H: Witzigerweise hatten wir das Thema auch, also den die Benennung für den Titel der Masterarbeit, weil ich es auch erst als SSI bezeichnet habe, aber wir sind davon abgegangen, zu dem Begriff dezentrales Identitätsmanagement.
A: Ja, ich glaube das ist auch viel, viel einfacher verdaulich. Also ich meine das ganze Thema Dezentralität ist für viele auch immer noch sehr abstrakt und was Identität ist, vor allem digitale Identität ist viele auch sehr abstrakt. Wenn man dann aber mit Beispielen kommt und gute Analogien schafft, dann kann man eher verstehen. Aber mit einem Begriff wie Self-Sovereign Identity, da fallen schnell erstmal die Klappen, da kommt sie garnicht mehr durch die Tür.
H: Das heißt, bist du der Meinung, dass vor allem auch öffentliche Institutionen zum Beispiel in der Rolle als Aussteller oder Überprüfer von Credentials dieses dezentrale Management übernehmen sollten?
A: Ja, das wäre optimal. Wir sehen jetzt aber natürlich, dass es gerade in der Verwaltung es ja immer so ist, dass bis da irgendwas sich ändert oder neue Verfahren adaptiert, es ewig dauert. Ich gehe also davon aus, dass wir da noch eine ganze Weile brauchen, auch wenn jetzt EU digital Identity Wallet mit eIDAS 2 und so alles kommt, bis dann tatsächlich staatliche Organisationen, Behörden, Ministerien oder wie auch immer, Credentials ausstellen, das wird noch eine Weile dauern. Was wichtig ist, ist, dass wir dieses Initial-Credential „Bürgeridentität“, also Personalausweis, wie auch immer man es nennt, in dem jeweiligen Land in der digitalen Repräsentanz haben, in dem Bundeskanzler Projektes Basis ID, also quasi erstmal eine Identität, mit der man dann mehr machen kann. Das ist ja sicherlich das, was als Erstes kommen wird, das Behörden noch zusätzliche Sachen, die nützlich sein können, ausstellen wird eine Weile dauern. Ich gehe daher davon aus, dass es privatwirtschaftlich organisierte Prozesse geben

wird, die bestehende Dokumente digitalisieren und als Credentials ausstellen, sprich du hast dann irgendeinen Nachweis, der von einem qualifizierten Service Provider digitalisiert wird und dir zur Verfügung gestellt wird. Das sehe ich eher passieren, als dass die Organisationen der staatlichen Organisationen direkt Sachen ausstellen. Wobei ich es natürlich sehr begrüßen würde, wenn das passieren würde und im Rahmen der Möglichkeiten, werden wir auch darauf einwirken. Also es wäre natürlich unglaublich nützlich, andere Sachen zu haben. Führerschein wird sicherlich kommen, da aber gucken wir mal in den praktischen Alltag, was kann man noch brauchen in Bewerbungsprozessen, polizeiliches Führungszeugnis, irgendeine Art von steuerlichen Nachweisen eine A1-Bescheinigung, um in Europa eine Geschäftsreise oder eine geschäftliche Tätigkeit auszuführen und so weiter. Das sind alles Sachen, die eher ein Volumen haben, mit denen man sofort was anfangen könnte. Vor allen Dingen im geschäftlichen Bereich und das wäre cool, wenn das passieren würde.

H: Deine Beispiele zielen jetzt hauptsächlich auf digitale Identitäten für Personen ab. Siehst du da auch einen Trend bezüglich IoT Geräten oder Smart Devices oder hast du da vielleicht sogar irgendwelche konkreten Vorstellungen davon?

A: Ja, was denn im im EU Kontext natürlich jetzt zusehends relevant wird und das ist auch ein Thema, wo ich mich sehr stark persönlich mit beschäftige, ist alles was zur Organisationsidentitäten betrifft, also sprich was haben eigentlich Firmen oder auch sonstige Organisationen, Vereine oder NGOs oder sowas, für Interaktionen mit Wallets, die dann in den Händen von natürlichen Personen sind. Also sprich mobile Wallets. Die der Bürger oder ein Kunde, oder wie auch immer der jeweils im Kontext genannt wird, hat. Also alles was, was eine Organisation machen muss in diesem Wallet Kontext ist super spannend. Das heißt also, da wird es noch viel geben. Das wird aber auch in den regulierten Rahmen dann stattfinden denke ich mal. Was da momentan zu wenig diskutiert wurde, ist das ganze Thema Maschinenidentität und IoT Devices. Ich glaube, dass viele, die jetzt in dem Bereich unterwegs sind, fachlich, da schon ihre eigenen Ideen und Fantasien haben. Ich glaube, dass einer der Volumenstärksten Bereiche sein kann für das ganze Thema, aber da ist bisher am wenigsten schon gemacht worden. Aber da sehe ich ein riesiges Potenzial, weil ich glaube, dass wir für Maschinen, die dann gegebenenfalls auch im im Autonomen, also physisch agieren draußen also sogenannte Cyber Physical Systems, dass die eine Art Identifikation brauchen, mit der Du die Authentifizierung oder autorisieren kannst. Und das wäre über Verified Credentials und Wallets und auch bei bei Sensoren mit wirklichen Mikro Wallets oder wie auch immer man die dann nennen

wird wunderbar abbildbar. Also ich sehe eigentlich für Self Sovereigin Identity, respektive decentralized Identity im Bereich IoT riesiges Potenzial, wobei es da bisher glaube ich nicht viele produktive Lösungen gibt.
H: Wahrscheinlich auch so ein bisschen ein Henne-Ei-Problem. Es müssten erst Lösungen entwickelt werden, die dann auch angenommen werden und umgekehrt, muss die Akzeptanz auch steigen.
A: Genau was du halt in dem Fall ganz stark irgendwann sehen wirst, ist der Move hin zu Zero-Trust Architecture, weil du hast halt gegebenenfalls draußen, wo die Sensoren oder die Aktoren sind, die die IoT Devices, die irgendwas machen, die werden vorsehen müssen, dass du dich gegenüber dem Gerät authentifiziert, über ganz leichtgewichtige Sachen, die direkt auch zwischen dem Gerät und Dir selbst passieren oder in deiner Wallet passieren und da hast du prinzipiell sofort ein Zero-Trust Modell und ich glaube, je mehr wir in diese Denke kommen - was ja auch ganz klar gewünscht ist - dann wirst du solche Mechanismen einfach haben müssen. Das wird einfach gar nicht mehr anders gehen.
H: Siehst du das dezentrale Identitätsmanagement für IoT Geräte auf derselben Stufe wie die für Personen, also dass zum Beispiel die Interaktionen zwischen Personen und Gerät auf Augenhöhe passiert, wenn beide eine Decentralised Id haben?
A: Ja, es ist ja letzten Endes erstmal eine Frage von Protokollen. Also was kann das Ding? Was kannst du mit dem Ding machen? Das ist eigentlich wesentlich. Ich glaube, dass das, was ich eben schon mal angedeutet habe, du wirst in dem in der Welt, in der wir uns jetzt rein bewegen, in diesem vernetzten Zustand, wo du Möglichkeiten hast, von jeglicher Art von Deepfake-Video Kram, du wirst in dem in diesem nicht physischen interagieren immer eine gegenseitige Authentifizierung machen müssen, damit du überhaupt sicher sein kannst, dass auf der anderen Seite der oder das ist, was du erwartest. Das heißt, du musst erst mal davon ausgehen, dass es nicht das ist bis, du eine Authentifizierung gemacht hast. Und die sehe ich über eine über eine Credential Logik extrem gut abbildbar. Das heißt, Augenhöhe. Wie auch immer. Also das ist eine Frage von Protokollen, was willst du erreichen und das meistens willst du erstmal Vertrauen aufbauen zwischen der dem Endpunkt mit dem du korrespondierst. Dass man dann natürlich noch ganz gut. Solche hierarchischen Konstrukte haben müsste. Wie ich delegiere, eine Art von Fähigkeit oder Berechtigung an jemand anders oder sogar an ein Gerät, das sehe ich ganz klar. Das heißt, dass du eine Delegation im Sinne von der hierarchischen Abhängigkeit schaffst. Das ist aber in den heutigen technischen Verfahren noch nicht so richtig drin. Das ist aber, was ich ganz

klar sehen würde, dass du eben die Möglichkeit hast, diese Delegating capabilities zu machen, auch über Credentials und das ist auch die richtige Logik.
H: Das ist sehr schöner, schöner. Punkt. Da kommen wir später noch drauf.
A: OK.
H: Ich würde kurz noch etwas über meinen mein Thema im Detail erklären, beziehungsweise Ausgangssituation schildern. Wir hatten uns, das sind meine Betreuer und ich. meine Betreuer sind, gerade beim Fraunhofer FIT aktiv und forschen da auch im Bereich dezentrales Identitäts Management. Wir hatten uns ein bisschen mit dieser Dreifaltigkeit Smart Vehicles, Smart Cities und. halt Identitätsmanagement befasst. Unsere Ausgangslage ist eigentlich der wachsende Trend, den wir jetzt erleben, dass immer mehr Städte zum einen digitaler werden, also auch ihre Infrastruktur digitalisieren, gleichzeitig aber auch mehr verstärkte Überwachung einführen im Sinne von Tracking von einzelnen Fahrzeugen, Tracking von ganzen Straßen, was das Thema ANPR, also Automated Numbers Plate Recognition ist da sehr groß, das praktisch Automatisiert jedes Fahrzeug, was sich in durch durch ein Kamera Bild bewegt erfasst, abgeglichen wird und identifiziert wird. Gleichzeitig sehen wir auch, dass es immer mehr Gründe gibt, warum das eingeführt wird. Also London ist ja sehr stark dabei, weil die sagen, Wir haben Umweltzonen oder wir haben Innenstädte, die sehr, sehr voll sind, weil einfach viele, viele Autofahrer durchfahren, und deswegen wird eine automatische Erkennung eingeführt. Um entweder Maut einzufordern oder auch wirklich zu sagen hier dieses Auto, da in diese Umweltzone zum Beispiel nicht einfahren. Unser Ansatz ist, das jetzt durch eine Art Framework in Richtung dezentral, das System und dezentrale Identität zu überführen, indem wir sagen. Wir möchten nicht, dass es eine zentrale Stelle gibt, die zum Beispiel ein Fahrzeug erfasst und vielleicht auch ein Bewegungsprofil erstellt. Sondern wir möchten, dass die Fahrzeuge in sich unabhängig und ja, die Identität selber verwalten. Ich komme gleich noch dazu, was ich damit genau meine, nämlich im Kontext zum Beispiel von Anwohnergebieten. Das ich zum Beispiel sage wie wird dann überprüft, dass ein Fahrzeug in einen Wohnblock fahren darf, ohne dass die ganze Straße dauernd blockiert, weil Autos die kürzeste Abkürzung nehmen. Wir hatten uns jetzt als Objective überlegt, was unser neues System praktisch als Ziel haben. Heute, das ist nämlich dieses Traffic Access Management ohne dauerhafte Kontrolle auch keine über dauerhafte Übertragung des Fahrt, also des Fahrzeug Standorts an irgendwelche Drittanbieter und was auch wichtig ist für uns ist zum Beispiel diese Übertragung. Von Zu-

gangsberechtigungen, wie gesagt, Anwohner oder zum Beispiel auch Parkplätze für Menschen mit Behinderung oder Einschränkung, dass diese tatsächlich auch nur genutzt werden können, wenn der Fahrer des Fahrzeugs auch tatsächlich diese Rechte dafür hat.
A: Ja spannend.
H: Und daraus ableiten wollen wir eigentlich ein bisschen diese Entkopplung von Fahrzeugidentität und Halteridentität bzw. Fahreridentität, weil wir dadurch sagen können, der aktuelle Fahrer ist eigentlich derjenige, der die Rechte besitzt, aber das gescannte Fahrzeug oder das getrackte Fahrzeug wird nur gesehen von den aktuellen Systemen.
A: Ja, cool
H: Und wenn wir das weiterspannen, können wir sogar sagen, wir können den Individualverkehr sogar etwas reduzieren, weil wir einfach sagen, es ist egal in welchem Fahrzeug ich mich befinde, ich als Fahrer übergebe praktisch meine Rechte oder übernehme auch meine Rechte mit ihnen das Fahrzeug, egal in welchem Fahrzeug ich gerade sitze. Das sind so unsere groben Objectives, die wir für unser Framework haben. Ich geh jetzt mal kurz ein bisschen ein bisschen das Framework ein, ist kein sehr kompliziertes Framework. Wir haben unsere klassische Aufteilung zwischen einer öffentlichen Einrichtung, welche auch immer das ist, es können auch mehrere sein. Wir haben natürlich einen Fahrzeughalter, der in irgendeiner Art und Weise mit einer Wallet Applikation ausgestattet ist, die er bedienen kann, mit der er auch seine Credentials verwaltet. Thema Basis ID ist es ganz klar. Das wäre schon was eigentlich am ehesten ausgestellt werden würde von so einer öffentlichen Einrichtung. Das Ganze natürlich gedeckt durch eine Art Distributed Technologie oder irgendeine Form von öffentlich und verifizierbaren Datenspeicher.
A: Genau, also wir reden aber von Verifiable Data Registry, ob das jetzt Blockchain, DLT oder ne klassische Datenbank ist, eigentlich völlig egal.
H: Ist eigentlich egal. Wichtig ist eben einfach nur, dass öffentliche Registry ist und dass die halt auch als Vertrauensanker dient in dem Kontext. Was wir jetzt aber zusätzlich noch ins Spiel bringen ist eben das Auto als Gerät, als Smart Vehicle in dem Kontext.
A: Mhm.
H: Hier spiegelt sich eigentlich das, was wir auch als vom Halter kennen. Nur haben wir jetzt zum Beispiel einen Hersteller, der dem Auto dann ausstellen kann. Du besitzt bestimmte Fahrzeugeigenschaften, bestimmte Emissionswerte, zum Beispiel die, von dem wir sicherstellen, dass sie einhältst, was dann das Fahrzeug an sich schon berechtigt, zum Beispiel eine Umweltzone zu fahren.

A: Sehr gut.
H: Hier ist eben, dass das Thema Delegation der entscheidende Punkt, dass ich, der Halter delegiert temporär muss ja nicht, muss ja nicht dauerhaft sein, diese Berechtigung an das Fahrzeug.
A: Genau. Wobei wir jetzt hier im aktuellen im Diagramm noch nicht drin haben, dass ich gegebenenfalls noch ein Anwohner-Credential könnte bekommen würde. Das heißt also, momentan implizieren wir einfach die Meldeadresse ist eigentlich der Bereich wo ich wo das Auto fahren kann soll, man könnte ja noch eine extra Stage reinmachen wenn es einen Anwohnerparkausweis bedarf, dann könnte ich den beantragen und der würde dann entsprechend die Zone definieren die ich da rein darf. Und die würde ich dann entsprechend an das jeweilige Fahrzeug, wo ich mich zu einem befinde, weitergeben.
H: Und wie gesagt, das muss nicht mal ein Anwohnerparkausweis sein. Das kann zum Beispiel ein Ausweis der Krankenkasse sein über eine über eine Behinderung, der Punkt ist, wenn wir einmal sagen, es gibt ein standardisiertes Verfahren oder ein standardisiertes Credential-Schema ...
A: Ja, okay.
H: ... dann ja beliebiges Credential ausgestellt werden.
A: Ja genau. Also was halt wesentlich ist, du hast es eben schon gesagt, dieses Thema Delegation. Wie würde ich jetzt für eine gewisse Zeit dem Auto diese Befähigung geben? Ne, also ich musste dann abgeleitet von dem was ich an Eigenschaften habe, die Daten weitergeben können über einen vertrauenswürdigen Weg. Das kann entweder sein, dass der quasi einen Proof-Request macht und die Daten abruft und das Auto damit das hat. Das wäre natürlich kryptografisch dann nicht revozierbar, weil es einfach nur das eine Abrufen von Daten, die ich dem Auto gebe. Das Thema Delegation, also im eigentlichen Sinne, würde sagen, ich gebe dem tatsächlich eine Art abgeleitetes, Credential und abgeleitete Attribute, die auch Kryptographisch verifizierbar sind vom Aussteller hin zu dem Auto für den Zeitraum, wo ich eben quasi der Besitzer des Fahrzeugs bin und dann darf es eben die Sachen. die mir zugeordnet sind. Das heißt, diese technischen Vorkehrungen, die wären entsprechend noch zu schaffen, und die ist momentan in dem, was wir an Credential-Logik kennen, noch nicht drin. Also der der Weg, wie man das heute machen kann, in einer Technologie die noch nicht so große Durchdringung hat ist diese Carry-Infrastruktur, wo du sogenannte Authentic Chain Data Containers hast, das ist so eine Art abgeleitetes Credential und damit könntest du sowas machen. Ja, aber das ist eigentlich genau der Weg wie man es machen wollen würde und das macht auch super Sinn.
H: Genau. Der letzte Schritt, praktisch als Verifizierung. Da gehen wir

dann wieder in den Bereich Smart City. Das wir wirklich sagen wir haben auch smarte Infrastruktur.
A: Ja.
H: Das kann alles Mögliche sein. Das kann eine Straßenlaterne sein, das kann eine Boden Welle sein oder so eine Boden Induktionsschleife, die dann eben einen Proof-Request stellt, den das Auto beantworten kann.
A: Ja super, ja. Macht super Sinn.
H: Der große Vorteil ist eben einfach. Wir haben diese Massenüberwachung nicht, wir haben auch keine, keine Kennzeichen Protokolle, wir können uns tatsächlich darauf konzentrieren, welche Credentials jetzt gerade im Fahrzeug vorhanden sind. Und kann sogar mit Zero-Knowledge Proofs Datensparsamkeit erreichen.
A: Genau, du kannst es wirklich ganz runterbrechen auf die minimalen Datensätze, die du brauchst. Also tatsächlich, wenn jetzt ein Credential hättest welches einfach nur die Zufahrtsberechtigung für den Bereich attestiert, könntest du einen Zero-Knowledge Proof auf das Credential machen und quasi keinerlei Informationen erheben außer die die Information: der darf da rein oder das Fahrzeug darf in diesem Bereich fahren, dann hast du wirklich eine absolute Datenminimierung.
H: Wir haben auch noch andere Ideen, das wir zum Beispiel sagen. Wir haben noch zusätzliche Fahrer. Im Fahrzeug, die dann alle ihr jeweiliges Credential übergeben könnten, dass das Fahrzeug dann auch als Sammelbecken. . .
A: . . . ein Bündel hat.
H: . . . genau so ein Bündel, ja, das war ja eine klassische Verundung, sag ich jetzt mal, an Rechten, dass man sagen von hat das eine Recht, von Passagier eins das andere Recht, von Passagier 2 und so weiter. Also die Erweiterbarkeit in dem Kontext wäre natürlich auch gegeben.
A: Ja, also da ist ja eigentlich einer der wesentlichen Vorteile, die ich immer gerne hin für Decentralized Identity. Du hast halt die Möglichkeit auf Basis von fließenden Daten Entscheidungen zu treffen und das kann alles Mögliche sein und es kann halt auch aus verschiedensten Quellen zusammenkommen und damit deine Entscheidungsbasis verbessern beziehungsweise auch diese Datenminimierung, also Datensparsamkeit maximal werten lassen, ja.
H: Wie würdest du grundsätzlich den Aufbau bewerten, wenn ich sage, das ist so die Idee von dem Framework was wir hier bringen? Rein von der Architektur her, wenn man draufguckt?
A: Kann man genauso machen. Also wichtig ist halt, du hast ja schon ein paar Mal gesagt, wenn es ein standardisiertes Verfahren oder Pro-

tokolle dafür gibt, dann kann man das machen. Ich glaube technisch eigentlich alles da. Müssen halt gucken, welche Protokolle dann in diesem physischen Raum greifen beziehungsweise welche Datenübermittlungsprotokolle. Da kannst du wahrscheinlich Bluetooth arbeiten, je nachdem wie dicht dran mit Bluetooth Low Energy, du kannst mit NFC arbeiten oder halt mit WiFi oder jetzt halt 6G oder sowas. Ich glaube das wird im Automobilsektor wahrscheinlich eher der Fall sein. Weil du ein bewegtes Objekt hast, was sich permanent gegen irgendwelchen anderen bewegten oder statischen Objekten authentifizieren muss. Also da muss man gucken, wie geht es tatsächlich am besten und die Credential-Logik is ja, das ist ja nur noch ein Add on dann über dieses Datenübertragungslayer und die kryptografischen Verfahren dazu sind ja alle da. Also kann man kann man super so machen.

H: Abgesehen jetzt von den ungeklärten Fragen, siehst du irgendwelche oder gibt es irgendwelche größeren Schwachstellen in dem Kontext, dass man sagt, das wäre jetzt irgendwo etwas daran würde, die Architektur scheitern oder das Framework scheitern?

A: Ja. Man muss halt gucken. Also das kann unter Umständen ja. Also was ich mir vorstellen könnte. Wenn das jetzt immer ist. Du musst halt da wirklich auch performante Systeme haben, weil wenn das jetzt alle machen wollen, dann funkst du die ganze Zeit und machst die ganze Zeit irgendwelchen Kryptografie-Kram sowohl in dem Auto, als auch in den in den, Ich sag jetzt mal Überwachungslogiken oder Ampeln oder was auch immer, das kann halt Performance Implikationen haben. Das muss man gucken, dass man das abstillt. Aber ich denke das ist das ist lösbar.

Und ansonsten sehe ich eher die Probleme in der Standardisierung der entsprechenden Daten. Das ist eher immer das Problem. Also dass wir das alles machen können ist total gut, aber du brauchst eben eine semantische Interoperabilität. Das heißt also, die Systeme, die miteinander da reden, die müssen wissen, über was sie reden. Das heißt, du musst hochgradig standardisierte Credentials haben, um die Entscheidungsfindung, also in einer minimalen Zeit zu machen. Ansonsten kannst nicht erst noch irgendwie negotiation oder sowas machen, sondern du musst eigentlich wissen, OK, ich mach jetzt die Abfrage auf dieses Credential und ich erwarte auch, dass da ist oder dass die Antwort gegeben werden kann und wenn nicht, dann darf eben nicht reinfahren. Das muss ja alles in einem Flow passieren.

Wir haben dann Dinge, die im physischen Raum sind, wo dann irgendwie auch zeitliche Abhängigkeiten und sowas sind. Das muss alles in einer gewissen Geschwindigkeit abhandelbar sein und du musst vor allen Dingen Wissen, was passiert in dem Fall wo der jetzt

nicht reinfahren darf. Blockiert er dann die Straße? Oder wie wird der geroutet? Du musst also quasi schon ne gewisse Dynamik vorsehen, bevor eigentlich dieser Fall eintritt. Ich muss entscheiden, der kann er da rein oder nicht. Also ich glaube diese Timing Sachen sind eigentlich die einzigen, die man wirklich gut beachten muss. Und diese semantische Interoperabilität. Das sind eigentlich die Sachen, die ich sehen würde, als wesentlich.
H: Abschließend noch die Frage, was siehst du so als größten, vielleicht auch politischen Blocker oder politische Gründe, die dagegen sprechen würden so einen ja Daten sparsameres Modell einzuführen, verglichen mit den bisherigen Systemen, die es gibt?
A: Also erstmal ein ganz grundsätzliches Verständnisproblem, dass sowas überhaupt geht, wie du es jetzt hier notiert hast oder wie wir es jetzt diskutiert haben. Das ist ja manchmal für Leute to good to be true. Geht das wirklich? Wie soll das denn funktionieren? Ich weiß eigentlich gar nichts, aber trotzdem ist die Entscheidung belastbar. Also das ist ja irgendwie so ein bisschen, klingt so ein bisschen nach einer Märchen-Story. Das heißt, da muss man ziemlich viel Education auf betreiben, damit erstmal verstanden wird, OK, das geht tatsächlich so und das ist auch, das ist auch wunderbar und funktioniert belastbar und ist keine Magie.
Das würd ich jetzt mal als global galaktischen Punkt sehen. Dann haben wir aber das andere Thema. Ja, wenn ich jetzt erst mal die Daten erfasst habe, das Rad wieder zurückzudrehen und zu sagen, wir wollen jetzt weniger erfassen. Das wird wahrscheinlich oft schwer fallen und sagen wir mal ganz ehrlich, ganz oft ist ja genau dieses Profiling und Tracking ein gewünschter Nebeneffekt, dass du halt im Sinne der Sicherheit oder der inneren Sicherheit ganz oft die Argumentation hast, ja, wir müssen ja alles tracken und alles machen, damit wir eben die Terroristen finden können. Weil die haben sich ja auch in irgendeinem Auto bewegt, was irgendwie ein Nummernschild hatte. . . .
H: „Denkt denn keiner an die Kinder?!“
A: . . . Das heisst ganz oft wird diese grobe Kelle. „Ja, wir wollen ja die Bösen fangen und ohne den Guten was zu tun“, genommen um zu sagen, aber die Überwachung ist absolut notwendig und das erleben wir ja auch in ganz vielen Stellen immer wieder.
Wir haben jetzt gerade mit dem Thema Chat Kontrolle, also Aufweichung der Verschlüsselung, Mechanismen ist genauso ein Thema, es geht ja nicht gegen die normalen guten Bürger, sondern es geht immer gegen die bösen Jungs. Aber dafür müssen wir natürlich die Sicherheit kompromittieren, von der ganzen Welt, damit es überhaupt geht. Und das ist natürlich eine absolute fadenscheinige Diskussion. Der

man stattgeben sollte, aber der man immer sagen soll. Die Sicherheit und die die kryptografischen Verschlüsselungsverfahren gehen vor und nicht wir weichen alles auf, damit es dann eben leichter wird, die bösen zu fangen. Also das ist glaube ich immer das Spannungsfeld, in dem wir uns bewegen. Immer was, wenn es um Vorratsdatenspeicherung oder Massenüberwachung geht, haben wir gleich diese Diskussion eigentlich wieder.
H: Ja, die Punkte seh ich ähnlich, auch mit dem Beispiel was du genannt hast. Chatkontrolle ist jetzt gerade wieder ein sehr aktuelles Thema finde ich. Du hast mir auf jeden Fall sehr geholfen, dass ich Input gegeben, finde ich super. Das würde ich auf jeden Fall auch verwenden im, Zuge der Arbeit. Die Idee ist, dass ich tatsächlich das Framework auch als iterativer Prozess, dass sich das ein bisschen weiterentwickelt. Das die ganzen Inputs einfließen und dann in der nächsten Version dann auch wieder evaluiert werden. Und so verfeinert man dann immer weiter diese Form von Frameworks
A: Genau sowas würde eigentlich auch in die Standardisierung gehören. Es werden jetzt die Automobilhersteller und so Anguckst und alles, die Beschäftigten sich sicherlich schon damit. Aber solche Frameworks, also auch gerade auch diese Datenstrukturen und so weiter, das würde ich in der Standardisierung und der internationalen Standardisierung sehen, und das hat sicherlich da genügend Platz um genau sowas da rein zu bringen.
H: Ja, also vielen, vielen Dank. Ich will dich gar nicht viel weiter stören.
A: Tust du nicht, hat mir sehr Spaß gemacht.
H: Ich bin auch. Sehr gespannt, wie sich das das Thema an sich weiterentwickelt. Also ich freue mich drauf, ich glaube das wird insgesamt eine schöne Technologie mit der man arbeitet, aber wie du schon sagst, da ist auch sehr viel Arbeit dahinter, dass auch aufrechtzuerhalten, denn ich glaube da ist sehr viel, auch Strömungen und Gegenströmungen in die andere Richtung.
A: Ja, passiert ja momentan sehr viel. Also ich glaube wir haben alle, als ich da 2015 mit angefangen habe, auch gedacht es geht alles bisschen schneller. Es ist schon ein echter Marathon. Aber jetzt hat es halt auf allen regulatorischen Bühnen die nötige Attention erlangt. Also ich glaube, wenn es jetzt nicht weitergeht, dann wüsste ich nicht. Was noch passieren sollte.
H: Hast du irgendwelche Fragen an mich oder an das System oder irgendwas in den Abläufen?
A: [Kopfschütteln]
H: Ja, das wars.
A: Ja, vielen Dank für die Einblicke. Klingt alles super spannend und

ich wünsche dir gutes gelingen jetzt mit der restlichen. Arbeit an dem Projekt.
H: Ja, vielen, vielen Dank. Ich lass euch auf jeden Fall wissen, wie es am. Ende ausgeht.
A: Unbedingt.
H: Dann sag ich dir auf jeden Fall schon tschüss.
A: Ja, ich danke dir. Und ja, wir sehen uns.
H: Alles klar, ciao.

TRANSCRIPT: EXPERT B (GERMAN)

H: Ja genau, also mich kennst du ja schon. Bist du vielleicht so gut und sagst mir was so dein, Schwerpunkt ist hier bei der Arbeit, bei [REDACTED] oder deine Rolle, so fürs Protokoll.
B: Alles klar. Genau. [REDACTED], CTO bei [REDACTED], angefangen im Jahr 2016. Damals schon schwerpunktmäßig im Identitätsmanagement unterwegs gewesen. In dem, was wir bei unseren klassischen, IAM Kunden so gemacht haben. Das heißt primär im Bankensektor unterwegs gewesen und dort klassische IAM Beratung gemacht dahingehend, dass eben. Verschiedenste Identität Töpfe gemeinsam gemanagt im Rahmen der Prüfungen [REDACTED] oder [REDACTED] und so weiter.
Ja, ist das entsprechend erfolgt. Bin dann seit 2019, eben auch in unserer SSI Themen mehr und mehr eingestiegen. Als innovatives Thema im Identitätsmanagement. Das bedeutet eben, wie kann ich im Zuge zunehmender Digitalisierung dafür sorgen, dass sich auch. Vertrauen in irgendeiner Form digitalisieren kann. Das bedeutet, wie kann ich Menschen und Maschinen etwas mitgeben, mit dem sie sich einmal als sie selbst identifizieren können, authentifizieren können und eben auch nachweisen können, welche Eigenschaften sie haben, um dann entsprechend in größeren Prozessen entsprechend ausgewertet zu werden, damit das auch automatisiert ablaufen kann.
Genau, bin daher von Anfang an dabei gewesen, kam auch auf die Idee, dass wir das Ganze mit dem Produkt untermauern sollten. Das Produkt, damals noch [REDACTED], ist auf einem meinem Mist gewachsen. Das wir eben gesagt haben, für unsere klassischen IAM Kunden, bringen wir sehr viel Klassisches IRM Know-How mit, wir wissen wie Berechtigungsmanagement funktioniert, Authentifizierung, Autorisierung auch mit der entsprechenden Governance dahinter und wir wissen auch, welche Tücken und Hürden es so dabei gibt. Und wenn wir ein eigenes Produkt aufbauen, wollen wir das gleich so aufbauen, dass wir gewisse Probleme, die wir aktuell heute schon in der Landschaft sehen, gleich mit beheben. Das Ganze ein bisschen moderner, agiler machen. Und haben uns deshalb dafür entschieden, einmal diese Enterprise- / Unternehmens-Identitätstöpfe mit so einer Technologie wie eben SSI verbinden zu können.
Dafür hatten wir damals [REDACTED] gebaut und von daher, da bin ich verantwortlich für all die Produkte, das bedeutet einmal für die für die Wallet Apps, die wir in diesem Zusammenhang erstellt haben, dann für [REDACTED] selbst und auch für die Branchenlösungen, die wir auf [REDACTED] aufgebaut haben, dazu gehören historisch einige Show Cases, die wir aufgebaut haben, dazu gehört aktuell noch

die Lösung: [REDACTED]. Und genau das beschreibt es so grob, was ich tue. Als CTO habe ich natürlich auch noch ein paar andere Aufgaben neben dem Tagesgeschäft und Produktgeschäft zwar auch eben für die für die IT Infrastruktur bei uns im Haus zuständig zu sein. Zu schauen, dass wir auch gemäß gängiger Standards unserer IT unter Kontrolle haben und auch entsprechende Services für Mitarbeiter anbieten, um das technisch ebenso zu untermauern, was wir in unseren Beratungsprojekten und bei unserer Produktentwicklung so benötigen.
H: Du hast ja schon gesagt, du bist sehr, sehr tief drin, sowohl im klassischen IAM Bereich als auch jetzt mit dem innovativen Thema wie SSI, wie bewertest du den aktuellen Stand von SSI? Also wie siehst du da die Annahme in der Bevölkerung oder auch von Seiten der Politik?
B: Also ich sag mal unabhängig von der Technik, hat, glaube ich, jeder verstanden, was damit verbunden ist - mit digitalen Identitäten. Das sowas notwendig ist und dass ich als Mensch so viele Interaktionspunkte habe, wo ich mich für Tickets auf einer Webseite registriere, wo auf meine Emails zugreifen, wo ich ein Haus bauen möchte und sowas. Ich habe immer wieder das gleiche Problem mit etlichen User Accounts, die ich mir in der ganzen Welt anlegen muss. Weil ich als Mensch für jeden neuen Service, der mich das erste Mal kennenlernt, tatsächlich ein ganz neuer Mensch, eine ganz neue Person. Und man von Grund auf ein Vertrauen in diese Verbindung reinbringen muss. Und dass das irgendwie nicht mehr zeitgemäß ist, hat glaube ich jeder verstanden, auch wenn das, was technologisch in SSI dahinter steckt und wie wir das Ganze lösen wollen, für die für die wenigsten tatsächlich begreifbar ist. Im Sinne von, dass jemand versteht, das ist genau die Technologie, die wir dafür brauchen.
Da sehe ich uns ein bisschen eben in einer Übersetzerrolle, um eben zu sagen: warum ist das genau die Art und Weise, wie man das tun sollte. Und da überzeugen wir eben mit Punkten wie dem Datenschutz, wo wir sehr auf Datenminimalisierung angewiesen sind. Das bedeutet, wenn ich schon in Interaktion trete mit anderen Services, mit anderen Menschen, dann möchte ich eigentlich nur die Daten dafür von mir selbst preisgeben, die dafür absolut notwendig sind. Ich möchte auch von meinem Löschrecht Gebrauch machen und von allem möglichen Anderen, was mir zusteht und das muss auch die Technologie gleich schon mitbringen. Das möchte ich nicht als manuellen Prozess noch irgendwo on top setzen müssen. Das sollte eigentlich nativ in solchen Technologien schon mit eingebaut sein.
Und daher ist SSI, in welcher Ausprägung auch immer - da gibt es Varianten, die in die Richtung Blockchain gehen, wo gewisse Sachen eben dauerhaft gespeichert auf einer Chain abliegen, was immer ein

Stück weit kritisch zu hinterfragen ist, ob das zum einen überhaupt notwendig ist und zum anderen, ob das entsprechend datenschutzkonform passieren kann. Es gibt aber genauso eben andere Formen digitaler Identitäten, auch im SSI Bereich, die ganz ohne dem Ganzen auskommen - und insgesamt muss man sagen, in diesem großen Feld tummeln sich 80 verschiedene Methoden, wie man alleine dezentrale Identifier bauen kann.
Es gibt zahlreiche Standards und Technologien, wie ich Nachweise erhalten kann und die präsentieren kann. Es gibt also sehr viele, ja unterschiedliche Ansätze und es hat sich noch nicht so richtig durchgesetzt, was das Ganze natürlich auch extrem schwierig macht, gerade weil man im Moment noch sehr viel auf Interoperabilität setzen muss, das Bedeutet wenn der eine in die eine Einrichtung baut und der andere die andere Richtung, dann wollen die trotzdem mit diesen Technologien gemeinsam sprechen können, sodass man das übersetzen kann. Das wird sich ein Stück weit relativieren, wenn sich die eine oder andere Technologie tatsächlich durchsetzt und man eben feststellt, viele setzen auf diesen einen Standard. Auch da kommen wir bestimmt später noch mal zu, was da in Europa gerade so stattfindet und inwiefern das maßgeblich das Ganze aktuell schon beeinflusst.
H: Wir haben gerade auch so der Trend, das gerade versucht wird auch durch W3Consortium ein bisschen zu standardisieren. Was sind die DIDs, was sind Verifiable Credentials und so weiter. Und das ist ja auch ein Trend für die Zukunft, hoffen wir mal. Aber würdest du eher sagen, du bist ein Befürworter davon, dass zum Beispiel öffentliche Institutionen oder auch Firmen vermehrt SSI verwenden oder auch eine Kompatibilität aufbauen, um diese Technologie zu fördern?
B: Ich bin auf jeden Fall dafür, das zu tun, denn die Alternativen sind alle aus meiner Sicht schlechtere Varianten ich habe Duplikate von Daten überall unterwegs, die sind nicht aktuell, die sind nicht authentisch. Jeder legt seine eigenen Töpfe an und die Art der Erhebung, die in der Regel dann auch noch über die großen IDPs erfolgt, von Google oder Microsoft oder ähnlichem, Facebook auch noch zu nennen. Das ist sicherlich etwas, was man als Anwender am Ende nicht haben möchte. Aus Datenschutzgründen und aus anderen Gründen, die mich eben gläsern für gewisse Unternehmen dastehen lassen.
Und ja, da hab ich zwar eine hohe Convenience, also ich kann das, was da angeboten wird, das macht Spaß zu benutzen, das bekomme ich meistens gar nicht mit, ich setze nur irgendwo einen Haken und automatisch können meine Daten schon zwischen ganz vielen Unternehmen hin und her wandern, aber in den seltensten Fällen ist das tatsächlich zu meinen Gunsten, sondern in der Regel viel mehr um eben auch ein Profit dahinter zu beabsichtigen.

H: Wie siehst du zum Beispiel das Thema Identitätsmanagement auf IoT-Geräten oder auf Smart Devices oder auf den immer schlauer werdenden Alltagsgeräten, die um uns herum sind? Siehst du da ne Kompatibilität oder bist du de, eher kritisch gegenüber?
B: Auch da ist es wichtig, dass wir wissen, wer mit wem spricht. Also auch der auch der Router, auch die Firewall muss genau wissen, wenn sie eigenständig im Internet gerade agieren möchte, ob wenn zum Beispiel Updates bezogen werden, um Sicherheitslücken zu schließen oder ähnlichem, das dort eben ganz klar eine Authentifizierung des Gegenübers stattfinden kann - da ist es gebräuchlich, da auch heute schon mit zertifikatsbasierte Lösungen, also Standard in der in PKI Welt mit x 509 Zertifikaten zu arbeiten und auch schon entsprechend die Integrität sicherzustellen.
Aber das geht natürlich mit SSI Technologie alles noch ein bisschen flexibler, das bedeutet da kann ich eben auch Eigenschaften den Geräten zuordnen und kann auch ganz individuelle Abfragen und Verbindungen zustande kommen lassen. Um da entsprechend ja gerade, was eben alles rund um Digitalisierung angeht, um Use Cases zu ermöglichen, die bisher eben mit solche stumpfen Zertifikaten, sag ich mal, nicht abbildbar waren.
H: Würdest du in Zukunft vielleicht auch sowas wie eine Augenhöhe sehen, dass ich als Individuum zum Beispiel Rechte oder auch Eigenschaften direkt an meinen, weiß ich nicht an meinem Fahrzeug oder an meinen Toaster übergebe, also davon wirklich sagt, die Individuen an sich oder die Entitäten an sich sind da auf einem Level. So als Zukunftsvision ist das valide?
B: Dass die Begrifflichkeit auf „einen Level heben“, finde ich jetzt noch ein bisschen schwierig, aber ja, also dass man die Brücke baut, dass man kommunizieren kann und dass man auf eine Art und Weise, egal ob Mensch-zu-Mensch, Mensch-zu-Maschine oder Maschine-zu-Maschine, dass da eine einheitliche Sprache gesprochen werden kann, die in einem Ökosystem zusammen agieren, verstehen können, das ist durchaus erstrebenswert aus meiner Sicht und ermöglicht eben viele neue Services eine, an die man ohne das nicht denken kann.
H: Siehst du da irgendwelche Nachteile oder fällt dir spontan irgendwas ein, was dem im Wege stehen könnte, so Zukunftsvision anzustreben?
B: Wir haben natürlich das Thema immer dann, wenn signierte Daten von mir preisgegeben werden. Das bedeutet, wenn ich etwas preisgebe, wo ich mit einer digitalen Signatur unterschreibe und der Empfänger das Ganze weiterverwenden könnte, habe ich natürlich auch da immer gewisse Angriffs Szenarien die ich im Kopf behalten muss. Denn mit diesen signierten Daten könnte unter Umständen, wenn die im

Darknet landen oder anderweitig verkauft werden, erheblich Geschäften mitgemacht werden, denn es ist kryptographisch prüfbar, dass diese Daten korrekt sind, das heißt, der Empfänger weiß ganz genau, was für Daten er da kauft und in dem Sinne ist das ein Stück weit als kritischer zu betrachten als wenn. Unsignierte Daten unterwegs sind.
Genau das ist ein Punkt, den man in dem Zusammenhang nennen kann. Die Frage ist, zwischen welchen Technologien ich mich entscheiden möchte. All diese Technologien sind natürlich anfällig für Sicherheitslücken und Schwachstellen. Von daher kann man da, gerade wenn wir jetzt nicht konkret auf einige Technologien eingehen, erstmal eigentlich nicht differenzieren, weil alle potenziell den gleichen Angriffsvektoren ausgesetzt sind.
H: Ich verstehe, lass mich kurz meinen Bildschirm teilen. Ich würde ein kleines bisschen auf unser konkretes Szenario von der Masterarbeit eingehen oder auf unsere Ausgangslage. Und zwar haben wir uns sehr mit dem Thema Traffic Monitoring und Access Management in der Smart City beschäftigt. Es ist ja schon relativ bekannt, dass es zum Beispiel Verkehrskameras gibt, die über automatische Nummernschilderkennung Fahrzeuge identifizieren können. Es ist bekannt, dass Fahrzeuge über SIM-Karten und GPS ihre aktuelle Position teilweise permanent auch übertragen an Hersteller oder wer auch immer sie gerade tracken möchte. Wir sehen, dass das ein Trend ist, der gerade zunimmt. Und gleichzeitig sehen wir auch, dass, beispielsweise in London, immer mehr Umweltzonen oder auch High Traffic Zones gibt, wo es darum geht, das es erfasst wird, wer in solche Zonen einfährt und ob er auch diese Berechtigung hat, da rein zu fahren. Und wenn man zum Beispiel in der Innenstadt von London unterwegs sein möchte, wird einem dann sogar automatisch schon eine Mautgebühr veranschlagt, weil man sagt, wir wollen das einfach reduzieren, dass diese Leute, diese, Wege nehmen. Und auch in Zukunft kann es ja durchaus sein, dass zum Beispiel auch Anwohnerareale oder Parkplätze für Menschen mit Beeinträchtigungen, eben in einer gesonderten Art und Weise, eine Authentifizierung oder Identifikation verlangen, um sie zu betreten. Das zum Beispiel auch nur derjenige, der mit einem Anwohnerparkausweis auch wirklich in die Straße reinfahren darf.
Was wir uns jetzt als Objective oder als Ziel vorgenommen haben, wäre zum einen mal zu sagen, OK, wir wollen natürlich eine Art Kontrolle bzw. Authentifizierung haben, allerdings ohne die ganze Straße zu filmen. Wir wollen auch gleichzeitig kein permanentes Senden des Standortes, des Fahrzeugs über die aktuelle Position und wir wollen auch, dass praktisch die Identität des Fahrzeugs von der Identität des Halters / des Fahrers entkoppelt und getrennt wird.

Sodass wir sagen können, ein Fahrzeug an sich hat vielleicht gewisse Eigenschaften, wie zum Beispiel die Emissionswerte um in einer Umweltzone zu fahren und der Halter hat gewisse Eigenschaften um eventuell Einwohner Straße zu fahren. Als finales Ziel daraufhin sogar möglich, so ein bisschen den Individualverkehr etwas zu reduzieren, weil ich dann einfach sagen kann, ich als Fahrer nehme einfach einen Mietwagen und übertrage dem meine meine Eigenschaften als Fahrer. Das sind Objectives, die wir uns als Ziel gefasst haben für dieses Framework, was wir uns ausgedacht haben.
Einfach nur, wenn du das so siehst, fällt dir spontan irgendwas ein, was da ja was sich da unlogisch anhört oder was dir spontan fehlen würde in den Kontext? Autorisierung von Fahrzeug und Halter?
B: Also erstmal finde ich das total interessant und nachvollziehbar wie man auf die Idee kommt entsprechend so etwas zu verbessern, weil eben hier haben wir auch wieder die Überwachung mit dabei. Das Tracking von GPS, Personendaten. Natürlich wollen wir davon weg, ja das Problem was ich immer bei solchen Lösungen ein Stück weit sehe, gerade wenn es eben um Maschinenidentitäten geht, hier haben wir wieder ein Fahrzeug was im Spiel ist. Wie identifiziere ich denn das Fahrzeug tatsächlich eindeutig? Was ist denn das, wo ich die Identität reinpacken kann, damit man die nicht einfach als Baustein rausnehmen kann und in ein anderes Fahrzeug reinpacken kann, denn genau das ist ja das Risiko, ich habe ein Fahrzeug mit einer gewissen Erlaubnis und wer hindert mich daran, diese Erlaubnis beliebig oft zu multiplizieren und andere Fahrzeuge mit der gleichen Erlaubnis auszustatten? Wie kann ich das verhindern, wie kann ich das kontrollieren? Ja, wie bekomme ich das mit. Wir sprechen da in der Regel von einer starken Hardwarebindung die irgendwie erforderlich ist aber auch da dieses Modul in was ich das rein packe, das kann ich vermutlich mit geringem Aufwand eben auch eine andere Stelle zumindest verlagern. Das heißt zwar, ich kann es nicht beliebig multiplizieren, aber ich habe trotzdem die Möglichkeit, eine andere Fahrgestellnummer plötzlich dann auch anzubringen.
Ja, das ist generell das Problem, auch wenn wir von Supply Chain Management Prozessen und ähnlichem sprechen, wenn Container versucht werden zu packen und so weiter. Der einfachste Fall, die bekommen einen QR Code oder einen Aufkleber. Ja wer hindert jemanden daran den Aufkleber abzumachen und dann den nächsten Container dran zu machen? Da gibt es natürlich Möglichkeiten gerade auch Schlüsselmaterial, was in Geräten angebracht wird, so dort zu platzieren, dass es kaputt geht in dem Moment wenn ich versuche dieses Schlüssel Material zu entfernen. Das ist sicherlich eine Variante, die ich hier nutzen kann.

Aber auch solche Sachen sind natürlich anfällig für Missbrauch und es ist oft einfach nur eine Frage der Zeit, bis auch so ein Verfahren wieder geknackt ist oder dass jemand einen Weg gefunden hat, wie man das nun doch übertragen kann ja auch dort, je nachdem wie man das macht, muss man schauen, ob Replay-Attacken unter Umständen möglich sind, das bedeutet ich schneide so ein Funksignal mit, was ein Auto mit zum Beispiel einer Schranke gerade so austauscht und wenn das. Keine gute, verschlüsselte Kommunikation ist und auch keine, die individuell in diesem Moment mit. Mit Schlüsselmaterial gemacht wird, was in dem Moment erzeugt wird. Dann laufe ich eben Gefahr, dass das jemand einfach sich mitschneidet und beim nächsten Mal selbst durch die Schranke fährt das.
H: Replay-Attacken, Ja.
B: Genau, genau das ist genauso das Thema, wo ich zwar gerne Lösungen für sehen würde, aber allein schon beim logischen drüber nachdenken oft recht schnell an den Punkt komme, wo ich mir denke, ja, so einfach wird es aber nicht.
Gerade beim Thema Fahrzeug ist natürlich total spannend, da ist ja auch das Thema Fahrzeug Lifecycle. So ein Fahrzeug wechselt ja auch mehrmals den Besitzer sowie andere Geräte auch. Ja, aber da hab ich letztendlich auch ein auch im Serviceheft, was oft noch manuell vorliegt. Ich hab die Historie der ganzen Besitzer und so weiter das sind schon Ereignisse, das ist eigentlich eine schöne Sache sowas zu persistieren und sowas eben Authentisch abzulegen über die komplette Laufzeit eines solchen Objekts. Und da arbeiten wir auch in [REDACTED] gerade mit [REDACTED] zusammen, die eben genau an so einer Lösung dran sind, eben Fahrzeugdaten beziehungsweise den Fahrzeug Lifecycle in einer Blockchain zu verankern, dort habe ich dann auch entsprechend Maschineninformationen - brauch mir wegen Datenschutz ein bisschen weniger Gedanken zu machen. Kann dann wiederum mehr die Vorzüge von der Blockchain nutzen, dass sowas tatsächlich nachprüfbar über eine gewisse gewisse Zeit und unveränderlich an einem Ort gespeichert ist.
Und ja, das ist entsprechend auch sowas, wo man schon sieht, dass solche Lösungen zum einen gefordert werden, zum einen aber auch schon entwickelt werden, aber auch da immer die Frage: Wo binde ich die Identität hin und ja, wie kann ich das Ganze sicher machen?
H: Ja, sehr interessant was du sagst. Das auch das Thema IT-Sicherheit, also wirklich physische Cybersicherheit da auch ein sehr großer Teil damit spielt.
Ich würde kurz nochmal auf das Framework an sich eingehen. So eine grobe Übersicht der Architektur, wie wir uns ungefähr gedacht haben. Das wird dir alles sehr bekannt vorkommen. Wir haben da, wir haben

uns natürlich sehr stark am klassischen SSI-Schema orientiert. Wir haben eine öffentliche Einrichtung, das kann ein Meldeamt sein, das kann eine Krankenkasse sein, das kann ja jede Form von Institutionen sein, die schon an sich ein sehr hohes Vertrauen genießt. Und die auch heute schon dafür zuständig ist, Identitäten auszustellen oder gewisse Eigenschaften auszustellen. Unser Fahrer in dem Fall oder der Halter des Fahrzeugs kann dann über seine persönliche Wallet-Applikation oder sein persönliches Wallet was er digital verwaltet, sich tatsächlich auch solche Credentials ausstellen und das Ganze eben über eine öffentliche registry oder halt einen Trust Anker in welcher Form auch immer das auch einsehen oder verwalten.
Gespiegelt wird das dann im Prinzip, indem wir uns das auch für unser Fahrzeug vorstellen. Das heißt, der Hersteller hat dann auch schon eine Möglichkeit, dem Fahrzeug ein eigenes Wallet zu füllen, mit bestimmten Credentials und bestimmten Eigenschaften. Sodass wenn dann der Halter wirklich einsteigt, er entweder temporär oder permanent, auch an das Fahrzeug übertragen kann. Und in dem Moment, in dem er dann mit dem Fahrzeug unterwegs ist und ein Credential, abgefragt wird, zum Beispiel über smarte Infrastruktur - das können Induktionsschleifen im Boden sein, oder es kann eine drahtlose Verbindung zu einer Lampe oder eine Ampel etc. sein.
Über diesen Proof-Request kann entschieden werden. OK, präsentiere ich dir jetzt Fahrzeug-Crednetials, präsentiere ich dir Halter-Credentials oder vielleicht sogar eine Kombination aus Eigenschaften von beiden Credentials. So dass eben diese Kontrolllogik dann in der Infrastruktur passieren kann. Das alles eben verankert hier auf dem auf den öffentlichen Registries oder auf den öffentlichen Datenstrukturen.
Das ist so der ganz einfache Case, wie wir uns das im Sinne vorgestellt haben. Natürlich geht das noch n bisschen tiefer. Natürlich haben wir noch Logiken, dann in der Infrastruktur drin, die Entscheidungen stattfinden, was passiert, wenn du nicht die Berechtigung hast, in ein Areal einzufahren, oder wie wird dann verfahren. Das sind aber eher auch politische Entscheidungen, die getroffen werden müssen. Jetzt so vom Groben, von der groben Draufsicht her würdest du sagen, dass erstmal valide die Architektur oder fehlt dir irgendwas ganz Wichtiges, was wir erstmal hier außer acht gelassen haben?
B: Macht total Sinn auf jeden Fall. Ich finde auch alle wichtigen Komponenten, die ich in einem Ökosystem brauche sind genannt und stehen dabei da auch auf jeden Fall zu erwähnen diese Trust Informationen die unten mit drin sind. Trust-Anchor, List of Trusted Agents, diese Trusted Registry, die ich letztendlich brauche, was in so einem Ökosystem in jedem Falle notwendig ist, damit ich weiß, wer sind

denn jetzt vertrauensvolle Issuer und Verifier.
Und genau da hätte ich vielleicht hier auch noch ne Rückfrage. Du hattest auch vorhin angesprochen, dass wir in so einem System davon sprechen, dass der Besitzer eine Befähigung, einen Nachweis dem Fahrzeug übertragen kann. Was auch eingezeichnet ist hier in der Slide. Das Fahrzeug wiederum kann dieses Credential offenbar selbst bei Präsentations wiederum vorzeigen. Ja, hat dort als Aussteller aber den Vehicle Owner registriert.
Ja, das heißt der Verifier würde einen Credential sehen, ausgestellt vom Vehicle Owner, da haben wir in der Regel ein Problem, weil ich genau da keinen Trust herstellen kann. Das bedeutet der Issuer ist in diesem Fall dem Verifier unbekannt. Das heißt, ich habe zwar, das Verifier Credental Ich kann sagen, dass das authentisch ist, aber die Informationen, die drin sind, hat mir jemand attestiert, den ich nicht kenne und den ich auch vermutlich nicht über die Trust Registry oder irgendwelche Trust Anchors abrufen kann.
Das ist ein Stück weit ein Problem, weil ich ja auch nicht so einfach Personen in einer öffentlichen Datenbank verankern möchte und da entsprechende Informationen ablegen möchte. Besser wäre. Wenn die Ausstellung dieses Credentials einer Verkettung oder einer Kaskadierung folgt. Das bedeutet, dass die Ausstellung dieses, also mal vielleicht ein Beispiel, der Vehicle Owner stellt, dem Fahrzeug eine Berechtigung aus, die er dir selbst weitergeben darf, um in ein bestimmtes Areal reinfahren zu dürfen. Dann darf ich das ja nur dem Fahrzeug ausstellen, weil ich wiederum selbst eine Befähigung dazu habe. Diese Befähigung habe ich vielleicht von einer Public Institution auf der linken Seite bekommen, die ich, die durchaus in der Trust Registry wieder drin steht und verankert ist. Das heißt, dort schließt sich wieder der Kreis. Das bedeutet, wenn ich das komplette Bild betrachte, habe ich wiederum Vertrauen in der ganzen Kette. Das erfordert aber, dass das Credential, was ich weitergebe eben diese Verkettung beinhaltet.
Und da ist mir im Moment nur eine Technologie bekannt, die in der Lage ist, sowas zu tun. Und das sind die Authentic Chains, Data Container, die ACDC Credentials. Tatsächlich auch Technologie, die gerade produktiv geht, wo wir die ersten Use Cases sehen, eben mit GLEIF, mit der Global Legal Entity Identifier Foundation, die das schon nutzt und einsetzt und promoted. So eine Technologie wäre aus meiner Sicht erforderlich, damit ich diese Spezialität in dem Use Case umgesetzt bekomme, weil ich sonst ein Problem mit der mit der Verkettung dieses Credentials habe.
H: Ja, das ist interessant. Wir haben immer diese Diskussion, wie du schon sagst, wer ist Aussteller und wer gibt praktisch per Delegation dieses Credential eben weiter und da kommen wir genau an solche

Punkte. OK wird auch kryptographisch festgestellt durch welche Stationen dieses schon gegangen ist. Also dass dann jeder ein bisschen Seine Signatur mit rein gibt und dass es dann zurück zu verfolgen bis an den eigentlichen Issuer.
B: Das sind letztendlich technische Implementierungsdetails. Ja, also auf der Slide würde ich jetzt einfach voraussetzen, dass damit gemeint ist. Das ich hier eine Vertrauenskette habe. Wie auch immer ich die gebaut habe und in dem Sinne ist, es ist eine vollständige Darstellung aus meiner Sicht, also kann so ein Prozess in einem Ökosystem funktionieren und ja, eben ablaufen. Das wäre ein erstrebenswerter Zustand, würde ich es mal nennen.
H: Das ist jetzt unser Basiskonzept. Wir haben uns auch Gedanken gemacht, dass wir das vielleicht sogar noch erweitern. Das wir jetzt zum Beispiel sagen, wir bringen noch einen Mitfahrer in das Fahrzeug. Der hat im ersten Moment erstmal die gleichen Eigenschaften wie auch der Halter. Das heißt, der hat selber eigene Berechtigungen, die er sich ausstellen lassen kann. Das können andere sein als der, der das können, aber auch ja von der Art her die gleichen sein, aber wenn bei dir jetzt eine Basis ID oder einen Personalausweis mit dem Wohnort oder der Straße ausgestellt bekommen haben. Das kann aber auch zum Beispiel sein, dass Passagiere die Berechtigung hat. Ich habe schon mal angedeutet, zum Beispiel auf einen Parkplatz für Menschen mit Beeinträchtigungen zu parken, und auch hier haben wir uns die Gedanken gemacht, okay. Es muss auch wieder eine Art Identitätsprüfung stattfinden, woraufhin dann dem Passagier erlaubt wird ein Credential an das Fahrzeug zu übergeben.
Ist etwas komplexer im ersten Moment. Hauptsächlich der Punkt Identitätsnachweis, das heißt der Passagiere muss dem Halter in irgendeiner Form nachweisen können, ich bin auch der echte Halter und auch diese diese berechtigungs Vergabe, dass der Passagier den Fahrzeug auch wirklich sicher übertragen kann. Weil sonst könnt ich ja hingehen, mich an ein Auto stellen und sagen ich. Geb dir jetzt ein. Cranchi weiß ich nicht was und das wird übergeben. Wie kritisch würdest du das? Würdest du diesen Fall betrachten? Also diese, diese Möglichkeit, dass jemand anderes auf seiner Eigenschaft Audits an meinem Fahrzeug übergeben. Könnte zum Beispiel.
B: Die Frage ist ja, gibt es einen Nachteil in dem Fall hier für den Passagier mit der Beeinträchtigung hat der einen Nachteil dadurch, wenn er das häufiger macht oder ist sichergestellt, dass ein solcher Berechtigungsnachweis eben nur einmal verteilt wurde. Ja denn sonst hindert in so einem Ökosystem ja niemanden etwas daran, diese Berechtigungsnachweise an beliebig viele Fahrzeuge zu verteilen und da vielleicht auch noch eine kleine Inzentivierung für zu bekommen. Ja,

das heißt, hier haben wir auch wieder das Thema, ja, Missbrauch in so einem Ökosystem. Ja, da muss man halt auf jeden Fall schauen, die Identifizierung gegenüber dem Fahrer, halte ich für weniger wichtig als gegenüber dem Fahrzeug dann tatsächlich. Der Vehicle Owner wird ja in direktem Kontakt zu dem Passagier sein, das bedeutet, da kann man heute auch über Proximity-Flows, das bedeutet einfach wenn die Handys nah genug in der Nähe sind, dann kann ich ja oder wenn ich den QR Code scannen von einem anderen Display, dann weiß ich wer mein Gegenüber ist und dann kann nicht allein darüber auch schon Prozesse anstarten ohne jetzt unbedingt noch einen Proof of Identity auf dem Wege einzufordern. Macht das Ganze natürlich noch mal ne Nummer sicherer, aber letztendlich würde es ja dem Fahrzeug keinen Nachteil bringen, wenn das Credential nicht durch den Owner verifiziert reinkommen würde. Ja, das heißt auch dieser Nachweis der ja auch, vielleicht Verkettet, wiederum abgeleitet mit drin steht vielleicht aber auch nicht, ist in der Form relevant, dass ich halt immer die Frage stellen muss, was könnte passieren, wenn ich sowas ermögliche? Wenn, wenn Angreifer jetzt tatsächlich mit drin sind oder einfach nur jemand, der ein bisschen Geld verdienen möchte. Mit so einer Sache.
H: Interessanter Punkt den Du sagst. Das sage, ich verleihe oder ich vergebe einfach meinen Behindertenausweis an jedem, der einen Euro dafür gibt und die dann alle auf dem entsprechenden Parkplatz direkt vor dem Eingang parken.
B: Richtig, je nachdem wie Datensparsam so ein System danach aufgebaut ist, kann der Verifier später auch gar nicht erkennen, wenn 2 Fahrzeuge reinfahren, ob der beeinträchtigte Passagier der dahinter steht hinter der Berechtigung, ob das tatsächlich der gleiche oder jemand anderes war. Ja das bedeutet, selbst wenn ich einen Parkplatz absichern möchte, könnten 10 Fahrzeuge darauf fahren mit der Berechtigung. Was an sich ja schon ein Problem darstellt. Ja, weil diese Berechtigung ist, also die die Person selbst, kann ja nur in einem Fahrzeug sitzen, aber ich kann noch nicht mal das als Verifier dann unterscheiden und müsste alle Fahrzeuge auf mein Gelände lassen. Ja und dann ja sowas halt entsprechend. Also da muss man sich ganz genau Gedanken machen, wie man hier das so abgesichert bekommt, dass ich wirklich nur den Use Case abbilde und das entsprechend da Restriktionen drauf habe. Zum Beispiel, dass ebenso eine Erlaubnis nur einmal vergeben werden kann und wenn die vergeben ist, dann muss ich sie erst wieder entziehen, bevor ich sie an ein anderes Fahrzeug übergebe. Das erfordert aber alles wiederum sehr viel zentrales Tracking, darüber. Das macht es wieder ein bisschen Datenschutzunfreundlicher am Ende. Genau das ist jetzt spontan was wir

hier wieder einfallen würde.
H: Es ist auf jeden Fall interessant was du sagst. Jedenfalls sehr viele gute Punkte dabei. Genau das ist schon gesagt. Auch das Thema Revozierung muss dann ja auch wieder kaskadiert erfolgen. Also entweder wenn die Institution sagt, ich entziehe dir das Credential, dann müsste das auch für die ganze Kette dann gelten und das muss auch irgendwo publiziert sein, dass dann der Verifier erkennt. Und ja, definitiv gute Punkte.
Wie siehst du das von der politischen Seite, sag ich jetzt malm was so die größten Blocker wären, um so ein dezentrales System, ein dezentral verwaltetes System auszurollen? Glaubst du da, ich meine für viele Städte oder auch für den für den Staat als solches wäre das eine Einschränkung, dann könnte er ja weniger tracken oder könnte ja weniger Daten erfassen. Glaubst du dass da, dass denen das denke stehen würde, dann eine dezentrale Lösung auszurollen?
B: Allein dadurch, dass weniger Daten getrackt werden. Das dürfte jetzt politisch kein Hinderungsgrund sein, sowas jetzt nicht einzuführen. Politisch ist jetzt natürlich eher relevant, wie sieht's denn hier in so einem System mit Gleichberechtigung aus und solche Sachen. Also wenn ich plötzlich so ein Ökosystem umstelle und plötzlich eine neue Technologie mit ins Spiel bringe, was mache ich denn mit Menschen die blind sind, die so ein Gerät vielleicht gar nicht bedienen können, ja wie inklusiv oder exklusiv Baue ich so ein System auf? Und was für alternative Prozesse muss ich gegebenenfalls berücksichtigen, damit ich auch jemanden, der das System nicht benutzen kann oder nicht benutzen möchte, trotzdem zu befähigen, da entsprechend integriert zu sein und das führt dann nicht selten dazu, dass der alternative Prozess in der Regel wiederum der Unsicherere ist.
Das haben wir bei den Impf-Nachweisen gesehen, wo zwar die digitalen Zertifikate da waren, aber trotzdem so ein gelber Zettel, den ich mir selbst im Drucker schnell ausdrucken kann, gleichwertig anerkannt wird. Das bedeutet, dass ich da natürlich auch auf der Verifizierer-Seite, je nachdem um was für nen Use Case es sich handelt, ich letztendlich wieder die gleichen Probleme wie vorher habe, weil die diejenigen, die mit dem Credential kommen, wahrscheinlich dann sowieso die vertrauenswürdigen sind und diejenigen, die Missbrauch vorhaben, dann den Papier Prozess wieder benutzen.
Ja und dann ist halt auch wichtig, was setzt sich hier technologisch ein. Und da gibt es verschiedenste Sachen zu betrachten. Wir haben den Stand der Technik in Deutschland, der oft Erwähnung findet, gerade in der Datenschutzgrundverordnung. Also ich muss ein System aufbauen, was den technologischen und auch Sicherheits- und Datenschutzstandards genügt, damit ich sowas betreiben kann. Das

muss geprüft werden, ob das in so einem konkreten Modell dann möglich ist. Und auch dann haben wir eben das Thema, was für Signaturen kommen zum Beispiel zum Einsatz. Und da ist man dann eben schnell in der Ecke, dass man auch schauen muss, ob die Algorithmen entsprechend beweisbar sicher sind, mathematisch geprüft sind und darüber hinaus schon großflächig im Einsatz sind, denn allein mathematischer Beweis zu einem sicheren Algorithmus reicht in der Regel gerade in einem Bundesamt für Sicherheit in der Informationstechnik in Deutschland nicht aus. Die Bestehen auch darauf, dass die Technologie schon eine gewisse Zeit lang in größerer Menge im Einsatz sein muss, um eben auch die Praxistauglichkeit da nochmal zu unterstreichen.
Und nicht selten gerade auch hier, wenn wir dann von Technologien wie Carry sprechen oder auch Blockchain verankerten Technologien oder auch ja modernen Verfahren wie Zero Knowledge Proofs formulieren kann, da ist sehr oft Kryptographie im Einsatz, die. Durch eine Prüfung durchfallen würde. Ja, und dementsprechend stellt das dann durchaus eine Hürde dar, dass ich da auch politisch nicht weiterkomme, weil ich entsprechend dem Regelwerk nicht gerecht werden kann, wie solche IT Systeme aufzubauen sind.
H: Ja, das sind super interessante Punkte. Danke dir dafür auf jeden Fall schon mal. Die Idee ist tatsächlich, dass all diese Interviews und auch diese Evaluation von solchen Familien wieder mit in den Entwicklungsprozess mit ein, die verfeinern dann immer weiter diese Arbeit, die wir hier machen, das am Ende das Framework auch irgendwann so stabil ist, dass man tatsächlich sagen könnte, das wäre, was man vielleicht irgendwann mal vorschlagen könnte und auch standardisieren könnte und vielleicht sogar implementieren könnte. Du hast mir auf jeden Fall sehr geholfen danke ich dir schon mal. Für hast du noch irgendwelche Fragen zum Ablauf und ich meine die Masterarbeit, wenn ich sie abgebe, werdet Ihr auf jeden Fall erfahren und ja, ich werde auch schauen ich dem laufenden was da noch kommt.
Und ja, wenn von deiner Seite aus noch Fragen sind, kannst du mir gerne noch. Stellen, weil ansonsten habe ich schon lange genug aufgehalten.
B: Alles gut. Kein Problem. Fragen erstmal nicht tatsächlich. Nur auch, ja vielleicht noch mal die Empfehlung, sowas eben auch noch in Einklang mit verschiedensten Bewegungen zu bringen, die es gerade EU seitig oder auch weltweit gibt. Also verschiedenste Ökosysteme, die gerade entstehen, vielleicht einfach mal zu bewerten, wo könnte sowas integrierbar sein, wo sieht man aktuell schon ne Bewegung genau in die Richtung um das ein Stück weit Einsortieren zu oder al-

lignen zu können. Oder auch am Ende zu beurteilen, was würde denn fehlen, damit ich dann genau so einen so einen Use Case damit umsetzen kann. Ja ich glaube das wäre das wäre sehr spannend nochmal entsprechend zu evaluieren, ob da vielleicht schon aktuell was in Aussicht ist, was genau sowas ermöglichen könnte. Genau, jetzt müsste ich tatsächlich jetzt geklingelt. Das passt.
H: Ja gut, ja, vielen, vielen Dank und ich wünsche dir schönes Wochenende.
B: Ebenso Hendrik, alles klar, bis dann ciao.

TRANSCRIPT: EXPERT C (GERMAN)

H: Okay das sieht schonmal gut aus. Und dann teile ich auch schon meinen Bildschirm. Siehst du meine Folien? Ja, perfekt läuft ja schon gut. Kurze Overview es geht einfach nur um das um die Fragen zum Framework. Ein bisschen was zum Setting vorneweg. Wir haben uns Gedanken darüber gemacht, wie wir heutzutage das Traffic Monitoring sehen und auch in Zukunft gestalten möchten. Und zwar sehen wir immer mehr. Das so ein Trend, dahin geht, mehr Straßenverkehrsüberwachung einzuführen. Hauptsächlich im Sinne von, was man hier auch sieht, durch solche Verkehrsüberwachungskameras oder auch anderen Technologien wie Geofencing oder, individuelles Tracking von Fahrzeugen. Wir haben gesehen, dass diese Form der Überwachung zunimmt, aber wir haben auch gesehen, dass es mehr Gründe gibt für diese Überwachung. Das heißt, es gibt immer mehr Städte auf der Welt, London ist ein sehr gutes Beispiel, wo solche Umweltzonen eingeführt werden oder auch „High Congestion Areas" die dadurch einfach steuern wollen und auch tracken und monitoren wollen, wieviel Fahrzeuge in Innenstädten unterwegs sind und eben, welche Auswirkungen das auf die Anwohner hat.
C: Geht's da jetzt eher um Statistiken oder geht es schon auch keine Ahnung, dann irgendwann mal darum feingranular je nach Tageszeit und Ort irgendwie Gebühren zum Beispiel zu verlangen für das Reinfahren und da ökonomisch das besser zu steuern?
H: Aktuell gibt es tatsächlich hauptsächlich um die Identifikation von diesen Fahrzeugen. Du hast schon völlig recht, die Hintergründe dazu sind meistens monetärer Natur. Das heißt, es werden entweder Mauten oder Zölle erhoben. Teilweise geht es aber eher darum zu verhindern, dass zum Beispiel Fahrzeuge durch Anwohnerviertel fahren, die da eigentlich nicht hingehören. Also wenn ich sage, ich möchte ein gewisses Viertel oder ein Quartier nur für Anwohner reservieren, dann möchte ich nicht, dass das eine Durchfahrtsstraße für LKW wird, weil das eben die kürzeste Strecke laut Navi ist. Und die Art und Weise, wie wir eben diese Fahrzeuge, welche auch immer das sind, identifizieren, ist jetzt erst der Kernpunkt von unserer Arbeit hier.
C: Ich mein, im Moment scheitert die Politik schon irgendwie, die Baustellen zu verpflichten, irgendwelche Geschwindigkeitslimits an als offene API zur Verfügung zu stellen. Also es geht wirklich um die Identifikation und dann bessere Methoden als Kennzeichenerfassung via Kamera wahrscheinlich, oder?
H: Ja genau das. Das ist aber der Grund Use Case sag ich jetzt mal.
C: OK, und warum braucht man eine bessere Erfassung als Kennzeichen? Das klappt ja eigentlich schon ganz gut, wenn ich so gucke an

Flughäfen mit Parkplätzen und so. Ich muss sellten mehr mein Park Ticket verwenden und reinstecken weil die schon wissen, dass mein Kennzeichen bezahlt hat. Was ist da die Motivation?
H: Unsere Haupt Motivationen ist es tatsächlich in erster Linie Bewegungsprofile im Allgemeinen. Also das ich sagen würde, ich kann ein individuelles Fahrzeug anhand der Kameras komplett nachverfolgen und Bewegungsprofile erstellen. In dem Fall auch über ja GPS Koordinaten, die über das Mobilfunknetz zum Beispiel gesendet werden, was ja individuell individuelles Tracking bedeutet. Der zweite Privacy Concern den wir haben, bezieht sich darauf, wenn wir zum Beispiel eine Kamera haben, die dauerhaft einen gesamten Straßenabschnitt überwacht und demnach auch Verkehrsteilnehmer mit aufnimmt, die eigentlich unbeteiligt sind für den eigentlichen Use Case. Also das ist zwar schön und gut, wenn meine Verkehrskamera mit Automated Number Plate Recognition alle meine Fahrzeuge scannt, aber es werden dann zum Beispiel auch Fußgänger aufgenommen oder werden Fahrer aufgenommen oder es werden. Ja, Passanten aufgenommen, die einfach nur über den Zebrastreifen wollen, der zufälligerweise in dem Fokus der Kamera liegt. Und das ist einfach ein Case wo wir sehen, OK, da könnt ihr noch mehr Datensparsamkeit vorhanden sein.
C: Also eher in Richtung Push, dass ich aktiv teile anstatt passiv alles aufzunehmen.
H: Genau das ist es, ja. Kurz ein bisschen zu dir, du hast ja schon Erfahrungen im Bereich dezentrale Identitäten. Wo ja auch die Reise bei mir hingeht, was die Forschung angeht. Wie lange bist du ungefähr in dem Bereich aktiv oder hast du da einen Schwerpunkt, den du dir da irgendwie gesetzt hast?
C: Die ersten Berührpunkte waren Ende 2019 in einem Projekt mit einem Automobilhersteller. Wo es halt eher Richtung Blockchain-basierte Identitäten ging, aber dann relativ schnell klar wurde, dass eine Blockchain halt im Moment, nur mäßig viel von Bedeutung ist für digitale Identitäten, wenn man irgendwie auf Privacy Rücksicht nimmt. Und seitdem ist es eigentlich so, neben Blockchain, mit der Schwerpunkt, den ich in meiner Forschung habe, insbesondere Richtung Privacy Enhancing Technologies, also wie kann ich unnötige zu kryptographische Korrelation bei digitalen Identitäten vermeiden und damit diese ganzen Überwachungs-Concerns, die man ja bei einer naiven Anwendung von digitalen Zertifikaten oder Blockchain basierten Identitäten hat, umgehen.
H: Da bist du schon sehr stark im Thema, auch was das Thema jetzt SSI, beziehungsweise dezentrale Identitäten angeht. Das sagt dir schon sehr viel. Das war nämlich so ein bisschen unser Ansatz, den wir mit unserem Framework verfolgt haben. Wir haben mehrere Ak-

teure. Wir haben einen Vehicle Owner, also jeder der ein Fahrzeug an sich erstmal besitzt und auch steuert. Und eine Public Institution, das kann eine Krankenkasse sein, wenn es um Behindertenausweise geht oder das können Meldeämter sein, wenn es um Adressdaten geht. Aber das können zum Beispiel mehrere Institutionen, die in irgendeiner Art und Weise der Öffentlichkeit zugänglich sind und auch ein gewisses Vertrauen genießen in der Öffentlichkeit.
C: Dieser Parkausweise für Behinderte, der ist tatsächlich in Frankreich auch schon umgesetzt worden meines Wissens.
H: Ja, da kommt auch ein bisschen die Idee.
C: Okay ja.
H: Tatsächlich sagen wir aber auch, es muss eine öffentliche Datenstruktur geben, die uns als Vertrauens dient. Wo wir auch Revocations mit steuern können. Und was auch wichtig ist, für eben diese Public Institutions, dass wir sagen, wir haben eine Liste of Trusted Agents. Das auch wir auch nachvollziehen können, dass der Aussteller von dem, von dem wir hier reden, dass er auch wirklich vertrauenswürdig ist.
C: Jawohl, soweit zu Use Case unspezifisch.
H: Genau das ist tatsächlich, mehr oder weniger, 0815 decentralized Identity. Das Ganze spiegelt sich ein bisschen dann auf der Fahrzeugseite. Wir sagen zum Beispiel, ein Autohersteller ist ein ähnlicher Aussteller von Credentials, der dem Fahrzeug zum Beispiel Emissionswerte oder grüne Eigenschaften ausstellen kann. Das zum Beispiel relevant für Umweltzonen.
C: Genau da hab ich ja auch bei diesen mobile Standards mitgeschrieben, in denen es dann um das legal Birth Certificate ging. In genau solche Stammdaten enthalten wären.
H: Und dafür haben wir uns überlegt haben, dass zum Beispiel gleichzeitig der Vehikel Owner durch eine Art Delegation oder Übertragung, auch eigene Eigenschaften von sich aus mit auf das Fahrzeug übertragen kann.
C: mhm.
H: Das heißt, das Fahrzeug an sich, man sieht es so ein bisschen Unterkomponenten, enthält ein Wallet, mit dem er seine Credentials verwaltet. Und diese Verwaltung kann auch dazu genutzt werden, das Delegations zu empfangen und auch im nächsten Schritt sag auch mit vor zu zeigen.
C: Delegation ist für dich eine Zertifikatskette oder weil die sind ja zum Beispiel jetzt in Aries/Indy noch nicht umgesetzt in der EU-Wallet sieht man auch nichts davon. Existiert überall als Konzept, aber nicht als Umsetzung.
H: Ja, genau. Also tatsächlich ich habe mich hauptsächlich mit den

ACDC Credentials ein bisschen befasst. Also diese Kaskadierung von den Credentials. Die aber glaub ich auch nicht hundertprozentig umgesetzt ist meines Wissens.
C: Ja, ich meine, wir kennen es von der Internet PKI. X.509 ist immer Zertifikatskette, aber für Personen halt noch nicht irgendwie verbreitet. Aber die Idee wäre sozusagen, wenn ich jetzt irgendjemanden Beweise, weiß ich nicht, ich darf Geld ausgeben im Namen meines Besitzers. Dann habe ich sozusagen meinem Auto was signiert, dass es über mein Bankkonto verfügen darf und dann zeigt mein Auto seine Identität vor und das ist von mir die entsprechenden Berechtigungen bekommen hat, oder?
H: So in der Art. Also der Bank Use Case ist vielleicht ein bisschen sehr speziell wegen der Drittparteien, die dann noch involviert sind, aber grob gesagt, wenn ich nachweisen kann, ich bin Anwohner in einem Quartier oder in einem Viertel und das Auto fährt rein, kannst praktisch der Infrastruktur beweisen, idealerweise per Zero-Knowledge Proof, ich darf auch wirklich hier drin sein. Und eigentlich ist der wirklich interessante Part dann im Fahrzeug, dass dann sozusagen ein Pool ist von verschiedenen Eigenschaften als Credentials ausgestellt, was ist dann mit der Infrastruktur kommuniziert. Und auch hier ist auch mal dargestellt. Diese Infrastruktur. In einer, sag ich jetzt mal Zukunftsvision einer smarten City, könnte das eine Ampel sein, das könnte eine Straßenlaterne sein oder auch vielleicht sogar eine physische Schranke, die auch Zugänge verwehrt. Auch als Trusted Trusted Agent System fungiert.
C: Okay und wie stellt ihr euch da die Kommunikation vor, also ist das dann über WLAN, Nahfeld oder wie würde das funktionieren?
H: Auch, das ist konzeptuell noch nicht hundertprozentig ausgearbeitet. Da ist eher die Frage nach den nach den Standardisierungsprotokollen, also ob ich jetzt sage, ich habe Induktionsschleife zum Beispiel das Auto fährt drüber. Ob das schon ausreicht, um möglichst schnell und möglichst performant dann diese Proof Requests zu empfangen und zu beantworten? Oder ob man sagen muss, OK, muss nach Form von drahtlos Kommunikation passieren, WiFi oder oder 6G oder was auch immer. Aufgebaut zwischen der Infrastruktur und dem Fahrzeug, dass eben dann dieser Austausch stattfinden kann oder dieser Handshake.
C: Mhm. Ja, da muss man halt sicherheitsmäßig ein bisschen aufpassen, dass halt auch wirklich du nur kommunizieren kannst mit Sachen, die in der Nähe sind. Das einmal dieser Nähe-Nachweis besteht, dass du halt über NFC, Bluetooth weiß, der Geier. In dem Prozess kannst du ja dann deine aktuellen IP Adressen austauschen und dann kannst du das ganze auch irgendwie über Wide Area Network machen,

aber muss man halt ein bisschen aufpassen. Damit man nicht immer mit allen Sachen interagieren kann.
H: Es gibt da mit Sicherheit mehrere Concerns. Wir hatten auch schon das Thema Bewegung in im Raum und auch wenn es mehrere Fahrzeuge sind, die da gleichzeitig interagieren wollen, das sind alles mögliche Concerns die dann auf die Infrastruktur dann einprasseln sag ich jetzt mal auf die Infrastruktur reagieren muss.
C: Das ist ja jetzt schon ein relativ dichtes Netz an Akteuren, denen ich da in der Stadt begegnen kann. Wie ist es denn auf der anderen Seite? Also du hast ja wahrscheinlich diese Man-in-the-middle-Themen bei digitalen Wallets mitbekommen. Ich brauche ja jetzt letztlich auch eine Liste von Trusted Verifiern im Sinne von, vielleicht nicht die Ampel direkt, aber die Ampel hat wahrscheinlich auch wieder irgendwie delegated Credential von der Stadt und die Stadt vom Land und das Land vom Bund, dass sie gewisse Kommunikation mit dir machen dürfen. Habt ihr das mal durchdacht, weil das ja doch eine relativ komplexe Infrastruktur wäre? Wenn das bis runter auf einzelne Ampeln oder so geht, die dann ja auch Schlüsselmaterial brauchen um dir zu signalisieren, du kommunizierst auch tatsächlich mit der Ampel.
H: Das ist auf jeden Fall ein valider Punkt. Wir haben es ein bisschen simplifiziert in dem wir einfach gesagt, es gibt irgendwo eine große Liste an Trusted Agents. Wahrscheinlich wie du sagst, über so eine Zertifikatskette wäre das am ehesten realisierbar. Vielleicht bist du da besser im Bilde ob es irgendwo bessere Wege gibt, so eine große Hierarchie von einzelnen Akteuren irgendwie abzubilden.
C: Ne, glaube ich nicht. Das Problem, dass ich nur sehe ist, du hast ja sogar bei den Fahrzeugen irgendwie relativ lange Entwicklungszyklen. Da wird jetzt irgendwie angefangen auch Hardware zu verbauen, die Schlüssel Material verwalten kann. Aber wenn man jetzt in Richtung Umsetzung denkt, dann hat deine Infrastruktur sowie die Ampel doch eine etwas längere Halbwertszeit und relativ selten Hardware an Bord, die Schlüsselmaterial verwalten kann. Das bedeutet also, wir reden da über Jahrzehnte, bis die entsprechende Infrastruktur aufgerüstet ist.
H: Ja also, Ampel ist tatsächlich ein Beispiel. Wenn ich das in einem Praxissystem oder in einem Praxisbeispiel mir vorstellen könnte, wäre das wirklich ein Zusatzsensor oder ein Zusatzgerät was da in irgendeiner Art und Weise mit aufgesetzt werden müsste. Diese Integration in die Infrastruktur wäre wahrscheinlich wirklich ein langfristiges Ziel, was in solche Akteure dann eingepflegt werden müsste.
C: Mhm, ja. Wenn du es halt nur obendrauf setzt, ohne es sauber zu integrieren, besteht halt schon eine gewisse Anfälligkeit für An-

griffe. Dann jemand das Ding abmontieren, woanders hin montieren, ein anderes Signal drauflegen um Verwirrung zu stiften und so weiter. Also müsst ihr mal drüber nachdenken, ob das so einfach nachrüstbar ist oder ob man das nicht wirklich stark integrieren muss und dann aber die entsprechenden langfristigen Implikationen berücksichtigen muss.
H: Aber ich finde du hast da schon guten Punkt angesprochen was das Thema Security angeht. Siehst du da sonst noch irgendwo Punkte die anfällig sind? Also vielleicht trennen wir noch mal zwischen zwischen Privacy und der tatsächlichen Security in dem Kontext.
C: Also das größte Problem, glaube ich, ist tatsächlich so diese Konsensthematik. Also wenn ich über die klassischen SSI-Anwendungsfälle denke, dann denke ich daran, dass ich einen QR Code scanne, gucke was wird von mir gefragt und dann bestätige, dass ich das freigeben möchte an die entsprechende Partei, die da auch namentlich genannt wird, typischerweise. Wenn ich jetzt Auto fahre und an eine Vielzahl von solchen Verifiern vorbeikomme, die alle mir eine Anfragen stellen und die Verifier, gehören im Zweifelsfall alle zu unterschiedlichen Organisationen. Dann muss ich ja letztlich einen Freifahrtschein an irgendeiner Stelle machen, so diese Daten teile ich einfach immer mit jedem, anders wird das ganze ja kaum zu managen sein. Dann ist die Frage, wieviel uns da halt dann unsere schöne Selective Disclosure und Co. noch bringt, wenn ich sowieso „by default“ immer alles mit jedem Teil, also ne übertrieben gesagt. Diese fein granulare Kontrolle, dass ich entscheide je nach Kontext und Empfänger welche Daten ich teile, die wird wenn ich eine Vielzahl von diesen Prozessen habe, und ich im Zweifelsfall auch noch konzentriert bin mit Autofahren, nicht mehr so einfach umsetzbar sein. Das heißt also, diese ganze algorithmische Kontrolle, was ich mit wem wann teile, wird wahrscheinlich sehr unübersichtlich. Also ich stelle mir das vor wie in config file, wo ich halt am Anfang, wenn ich das Auto einrichte, sage mit Ampeln teile ich das, mit diesen Teilnehmern teile ich das, und so weiter. Ob das besonders nutzerfreundlich ist, weiß ich nicht und dann geht es uns wie mit den Cookies einfach immer auf alle akzeptieren. Und dann haben wir am Schluss zwar technologisch Privacy und Zero-Knowledge an Bord, aber wenn ich sowieso alles mit jedem Teilen bringt uns herzlich wenig.
H: Ja, man kann höchstens sagen, ok durch Zero-Knowledge Proofs ist eine gewisse Sparsamkeit da der Daten. Aber klar, also man müßte eigentlich per Default auf Auto answer oder Auto accept das so einrichten, dass das auch automatisch akzeptiert werden, wenn es soweit ist.
C: Und weil ich wahrscheinlich keine Lust habe, dass am Anfang mal

auszufüllen, je nach Art der Infrastruktur folgende Attribute sag ich einfach, OK mit der jeder Infrastruktur teile ich alle Attribute die sie haben will und spätestens dann ist das mit dem ZKP halt irgendwie naja eigentlich hinfällig, weil dann vermeide ich vielleicht noch ein paar schöne eindeutige Kryptographische Identifier, aber wenn sowieso mein Kennzeichen oder meine Vehicle Identification Number oder sowas übertragen wird, dann ist es auch ein unique Identifier. Wenn ich tracken will, brauche ich das ja auch zu einem gewissen Grad und dann fragt halt einfach jeder damit danach, weil er das kann. Und vielleicht kann man das irgendwann monetarisieren.
H: Ja, wobei man sagen muss, da gehen wir schon in eine andere Richtung rein, wenn wir sagen: „Was wäre denn ein Interesse der Parteien, da mehr Daten zu sammeln?“ Also natürlich muss man da sagen, da haben die Akteure, die jetzt auch schon den Verkehr überwachen, ein großes politisches oder finanzielles Interesse, da eine möglichst weite Überwachung auszurollen. Die Frage ist eher, wie kann man dem entgegensteuern? Also es muss im Prinzip technische Möglichkeit geben, da diese Datensammelwut ein bisschen einzudämmen. Deswegen war im Prinzip die Überlegung, dass man solche eindeutigen Identifier wie ein Kennzeichen oder so Fahrzeugidentifier, dass man die gar nicht gar nicht ins Credential packt, sondern wirklich eher so Fahrzeugeigenschaften, die dann an sich per ZKP übertragen werden.
C: Die Frage ist halt, wie viele Fahrzeugeigenschaften brauche ich in einer gewissen Zone, um eine eindeutige Identifikation vorzunehmen? Erfahrungsgemäß braucht man halt nicht besonders viel. Also irgendwie, gab es mal ein lustiges Experiment in den USA, in den, ich glaube, späten Achtzigern, wo du letztlich über 80% der Leute eindeutig über Geburtsdatum, Regionen und Geschlecht identifizieren konnte ist. Also du brauchst nicht furchtbar viel.
H: Mhm, auch ein guter Punkt diese statistische Korrelation, ja.
C: Postleitzahl wars glaub ich auch noch.
H: Das ist ein guter Privacy Aspekt auf jeden Fall.
C: Also da bräuchte man wahrscheinlich eine gute Vorstellung davon, wie man bei dieser hohen Anzahl an unterschiedlichen Identity-Proofs, wie man da Privacy nicht unter den Tisch kehrt, obwohl man da ein tolles Fotographisches Framework hat.
H: Siehst du irgendwo noch Schwachstellen in Bezug auf Security, du hast einen sehr guten Punkt gebracht, was die Kommunikation mit der mit der Infrastruktur angeht. Aber so Sachen zwischen Owner und Vehicle oder zwischen Institution und Owner, meinst du da gibt es noch was?
C: Ja, also. Also vor allem halt dieses Thema Identifikation des Verifiers, um Man-in-the-middle auszuschließen. Und das benötigt let-

ztlich eine sehr fein granulare PKI und Zertifikatsinfrastruktur auf der Infrastruktur Seite, die halt heute nicht existent ist. Also streng genommen müsste ich halt irgendwie jeder Ampel, Schlüsselpaar geben und dann noch ein entsprechendes Zertifikat und dann ist halt auch die Frage, also wenn das so weit verbreitet ist, ob das nicht auch anfällig ist? Also im Zweifelsfall wenn ich irgendwo was ausspähen möchte, alle Ampeln im Griff zu behalten wird schwierig. Dann bau ich halt bei einer entsprechenden Kommunikationsmodul mit dem Schlüssel aus und stelle es vor meine Haustür, wenn ich tracken möchte, was der Nachbar wo unterwegs ist. Also das System wird halt dadurch sehr groß, sehr komplex und damit notwendigerweise fehleranfällig.
H: Auf jeden Fall interessanter Punkt.
C: Also das mag in einigen Anwendungen durchaus funktionieren, aber man sollte sich halt zumindest bei sagen wir mal sehr kritischen Themen, wie jetzt zum Beispiel in der Bezahlung, muss man das vermutlich schon auch einschränken, um das halbwegs sicher zu halten. Also manche Daten zu teilen ist wahrscheinlich nicht besonders schlimm, andere wiederum, die sensitiv sind, die möchte man halt nicht so oft mit so vielen Parteien by default teilen. Weil dann halt also im Zweifelsfall reicht halt eine, die malicious ist und die einen schönen Replay macht. Und dann bist du dein Geld los.
H: Ja, also Replay-Attacken sind tatsächlich auch was, was uns schon gesagt wurde in den Interviews, dass das auf jeden Fall ein kritischer Punkt ist für die Kommunikation.
C: Also im Prinzip ist ja Replay mit SSI adressiert, aber nicht wenn der Verifier bösartig ist. Dann kann es dir passieren, dass er dir die nonce weiter spielt und deswegen solltest du halt zweimal überlegen, wenn dein Auto jetzt irgendwie über dein Konto oder deine Kryptowährungs-Wallet oder sowas verfügt, weil da halt schnell auch mal was schief gehen kann. Das heißt also, da willst du dann im Zweifelsfall halt schon eher nochmal eine direkte Kommunikation mit weiß ich nicht, „Paypal“ oder „Easy Park“ und vielleicht nicht mit der Ampel die das Geld empfängt. Also da muss man dann wieder über eine gewisse Zentralisierung nachdenken, zumindest auf Verifier-Seite, dass die Kommunikation vielleicht angestoßen wird durch die Infrastruktur, aber das halt der Haupt Workflow schon eher über eine neue vertrauenswürdige Organisation läuft als über irgendein Edge-Device mit fragwürdigen Vertrauensniveau. Ne, also so ähnlich wie, halt keine Ahnung, du stehst Mitternacht an so einer automatischen Tankstelle und dann zieht vielleicht dieses Ding wo du deine ec Karte reinschiebst nicht ganz so vertrauenserweckend aus oder geklebt, ja...
H: Immer dran wackeln, ja.
C: ...sowas kann dir halt passieren. Und deswegen willst du sowas

im Zweifelsfall halt lieber über eine Organisation, die direkt spielen mit einigermaßen hohem Vertrauensniveau. Und am Anfang wird nur dieser Kanal aufgemacht, der dich in die richtige Organisation leitet, also sprich „Paypal" oder keine Ahnung was.
H: Ja, gute Punkte. Die du da anspricht auf jeden Fall. Wir haben uns noch bisschen Gedanken gemacht ob man den Use Case, den wir hier haben ein bisschen erweitern kann. Wir haben zum Beispiel gesagt, es gibt noch sowas wie ein Mitfahrer, der nochmal andere Eigenschaften besitzt als der der Fahrzeugführer oder Fahrzeughalter. Der auch über eine ähnliche Art und Weise seine Credentials bekommt. Und es jetzt Möglichkeit, gibt zum Beispiel auch zu sagen, der Mitfahrer kann zusätzlich seine Credentials mit an das Fahrzeug übergeben, das ganze temporär beziehungsweise auch nur limitiert. Das nur einmal an das Fahrzeug ausgeliehen, kann zur gleichen Zeit. Das ist so der Extended Use Case.
C: Kann man sich schon vorstellen. Ja, bräuchte man halt irgendwie guten Anwendungsfall, wo das auch sinnvoll ist. Sonst kann ich ja sowohl mit einem sehr kurzlebigen Zertifikat ne, also Delegation wird Expiration für, weiß ich nicht eine Stunde, man könnte sich mal noch überlegen, ob man da auch noch irgendwelche Proximity-Nachweise mit rein bekommt. Also das es auch nur funktioniert, solange sich der Passagier innerhalb des Fahrzeugs oder so aufhält. Aber das wäre dann schon außerhalb vom Standard SSI Protokoll ne dass man sagt, OK, im Zweifelsfall fragt dann das Fahrzeug noch mal nach einer Unterschrift vom Passagier um irgendwas zu betätigen.
H: Ja genau, über solche Proximity Lösungen hatten auch schon nachgedacht, dass wir sagen, sobald sich das das Handy oder das Gerät vom Passagier aus dem Fahrzeug heraus bewegt oder weiter als ein Meter Abstand, dann wird halt wieder Revoked, dann wird automatisch wieder gelöscht aus dem aus dem Fahrzeug-Pool.
C: Ja, das wird halt schwierig, weil das nicht kontrollierbar ist. Also wenn der Passagier dem Autoeigentümer oder dem Auto traut ist sowieso alles easy, aber erzwingen kann er es halt nicht, dass es gelöscht wird. Das heißt also für die Sachen, bei denen du sagst, vielleicht will ich die auch schon früher als eine Stunde entziehen. Das musst du halt dann entweder aktiv revoken als Passagier oder sagen, OK, ich möchte bei jedem Vorgang, den meine Credentials verwendet, vielleicht doch mal selber bestätigen, dann würde ich aber halt wahrscheinlich nicht mal an das Vehicle delegieren, sondern dann würde das wirklich nur connection zu mir haben und im Zweifelsfall halt an mich weiter verweisen für den entsprechenden Identitätsnachweis.
H: Das praktisch das Vehicle einfach den Proof request weiter reicht

an den entsprechenden Besitzer, oder?
C: Genau. Und dann geht genau da könnt ihr mal so ein bisschen nachdenken wie das ist. Ich meine, letztlich haben wir so ein bisschen ähnliche Thematik, wo dann auch Proximity mit rein spielt bei so Terminals für deine eID. Da spielt das Auto sozusagen einfach nur den Kommunikationskanal, der sicherstellt, dass du auch tatsächlich im Auto bist und die Kommunikation findet aber direkt zwischen dem Passagier und dem Verifier statt. Mir ist jetzt aktuell auch keine SSI Implementierung bekannt, die irgendwie Credentials von mehreren Parteien kombiniert. So dass ich dann sozusagen weiß, ok ich, ich stimme jetzt nur zu weil der andere im Auto auch schon zugestimmt hat oder dergleichen. Also ich glaube das ist schon außerhalb des Standard-Workflows.
H: Ja, was eine Überlegung wäre. Man delegiert von mehreren Quellen seine Credentials and das Fahrzeug und dann wird einfach nur Vorhandensein geprüft. Das ich sage, „ja das ist vorhanden", „das Credential ist nicht vorhanden" und dementsprechend. Wird dann ein Schluss daraus gezogen wer auch immer der Verifier, dann ist in dem Kontext.
C: Okay.
H: Ich muss noch auf dem Fragebogen kurz gucken, denn wir haben schon sehr viel besprochen davon. Meinst du denn, deiner Einschätzung nach: diese Identitäten lassen sich entkoppeln von Fahrer und Fahrzeug? Was ich damit meine ist, wenn ich heutzutage mit meinem Auto unterwegs bin. Mein Kennzeichen wird gescannt und das wird zum Beispiel in Flensburg oder wo auch immer im zentralen Fahrzeugregister der Kraftfahrtstellen überprüft. OK, dieser Halter mit diesem Fahrzeug. Es ist eindeutig hinterlegt und eine Einheit. Meinst du, das ließe sich durch so ein dezentrales Fremdwort entkoppeln, dass ich sagen kann, ich habe Fahrzeugidentitäten und ich habe Personenidentitäten und die müssen nicht läufig zusammengehören?
C: Also ich sehe jetzt nicht, wie es stärker entkoppelt werden sollte, als es heute schon ist. Weil rechtlich, also diese Trennung ist ja meistens irgendwie rechtlicher Natur, es im Zweifelsfall egal Ist mit welchem Auto ich fahre, solange ich Punkte sammle. Das Auto hat heute ja auch schon eine eigenständige Identität, ne WIN Nr. im Zweifelsfall. Im Fahrzeugbrief bin ich sogar noch als Halter eingetragen, aber ich habe irgendwie noch das Certificate auf Conformity und so, also de facto haben wir auch heute schon Identitätsdaten des Fahrzeugs. Der TÜV klebt auch am Fahrzeug, nicht am Eigentümer. Entsprechend haben wir in erster Linie die Digitalisierung von diesem Ganzen. Identitätsdokumenten, die wir auch heute schon für das Fahrzeug haben. Also sehe ich da jetzt eigentlich. Nicht direkt ein Unterschied.

H: Also ich glaube der Hauptunterschied wäre dann: Wir haben Sachen wie das eben gewisse Fahrzeugberechtigungen nicht mehr direkt am Fahrzeug fix angebracht oder vorhanden sind ja wie die Umweltplaketten oder Anwohnerausweise und sowas, sondern dass das inzwischen als Credential beim Halter oder beim Mitfahrer liegt und das Fahrzeug im Prinzip so ein Behältnis dafür ist. Meinst du, dass, das würde sich so umsetzen lassen?
C: Ist es das nicht heute auch? Also ich könnte ja im Prinzip meinen Parkausweis auch mitnehmen in meine Wohnung. Also, wenn ich gerade nicht parke, nehme ich mit und wenn ich parke, dann leg ich wieder ins Auto, weil ich ihn gerade brauche. Und Zweifelsfall habe ich halt jetzt Kopie bei mir, wenn du möchtest und dir eine Kopie klebt im Auto und die andere ist in meiner Brieftasche, falls ich sie mal brauche, ohne dass ich Zugriff aufs Auto habe. Also vielleicht allgemein die Verfügbarkeit halt ein bisschen erhöht und die Flexibilität. Ob es wahnsinnig viele Use Cases gibt, dafür weiß ich nicht. Aber ich sehe jetzt keinen Paradigmenwechsel.
H: Ja, das war noch ein Gedanke, den wir ein bisschen verfolgt hatten. Auch zum Teil von unseren unseren Design Objectives, die wir uns hier überlegt hatten. Das wir sagen dann durch dieses Framework liese sich eben dieses permanente Monitoring bisschen reduzieren. Das du auch keine dauerhaften Profile der Fahrzeuge an sich hast. Und eben noch so ein bisschen als Folge von dem von der Prämisse, diese Entkopplung. Dass man sagen könnte, jetzt bin ich zwar durch den Besitz meines, meines Fahrzeugs ein bisschen daran gebunden und ich könnte zum Beispiel sagen, mit einem dezentralen Framework bräuchte ich eigentlich gar keinen, gar kein festes Fahrzeug, sondern könnte mir beliebige Fahrzeuge temporär leihen oder sie könnten meinen Besitz übergehen um dann meine Berechtigung dahingehend übertragen. Und am Ende, wenn ich, wenn ich wieder aussteige, würde ich, würde ich dann eine Berechtigung einfach wieder mitnehmen bis ich ins nächste Fahrzeug steigen.
C: Ja, das ist diese Kopien-Geschichte. Ich muss halt nicht abkratzen und wieder einkleben, sondern ich kann es flüssiger mitnehmen. Bei Bedarf ja.
H: Ja, das wären so die die Objectives, die wir uns gesagt haben. Siehst du da irgendwo wie es nicht funktionieren sollte, oder? Glaubst du das einzige dieser Objektive nicht erfüllt werden könnte?
C: Ja, also beim rechten [im Bild] gehe ich glaube ich mit. Dass wir das leichter entkoppeln und leichter auch portable machen, mehr oder weniger die Eigenschaften sowohl für unterschiedliche Nutzer des gleichen Fahrzeugs als auch für unterschiedliche Fahrzeuge des gleichen Nutzers. Bei den anderen zwei Sachen bin ich mir nicht sicher. Also

letztlich: Überwachung ist ja in der Regel etwas das nicht opt in ist. Das heißt also was jeder über sich ergehen lassen muss. Und wenn ich halt jetzt auf ein Kommunikationsprotokoll umstelle, das nicht irgendwie eine gewisse Gegend wacht, sondern darauf wartet, dass das Auto mit mir kommuniziert. Ich habe immer die Möglichkeit, keine Ahnung, zu welchen faradayschen Käfig um meine Antenne herum und dann kommuniziert das Auto mit keinem mehr und existiert nicht. Also ich weiß nicht, inwiefern man dann wirklich auf so kamerabasierte Überwachung verzichten kann. Mithilfe dieses Ansatzes. Mag sein. Also ja, ich habe keine permanente Übertragung von den von der Location. Andererseits, ich habe ja die Location von meiner Infrastruktur und wann immer die mit meinem Fahrzeug kommuniziert und wie gesagt, Tracking ist wahrscheinlich relativ einfach, selbst wenn ich keine globally Unique identifiers hab basierend auf einer größeren Anzahl von Attributen bin ich schon relativ eindeutig normalerweise identifizierbar und dadurch weiß ich nicht, ob das Profiling dadurch wirklich stark reduziert wird. Für mich würde jetzt vielleicht weniger aus der Privacy-Motivation ein Schuh, sondern eher aus wie kann ich digital verifizierbar machen wer da gerade ist? Warum weiß ich nicht. Irgendwelche Rabatte, Bezahlungen, Berechtigungen und so weiter nachzuweisen, weil da möchte ich wahrscheinlich nicht das im öffentlichen Register ist das mein Kennzeichen geheftet ist. Für mich eher das Thema Integrität, wahrscheinlich als Privacy, das da überzeugend ist.

H: Du hast es schon ein paar Mal gesagt, aber eben auch. Das Überwachung, hauptsächlich opt in und nicht opt out ist. Glaubst du denn, dass politisches Interesse überhaupt da ist um auf ein Datensparsameres Modell der Verkehrsüberwachung umzusteigen oder glaubst du, dass es politisch überhaupt nicht gewollt?

C: Also ich denke du würdest schon Fürsprecher finden. Aber ich glaube, wir haben aktuell größere Baustellen an anderen Bereichen, in denen diese Privacy-Diskussion läuft und wo sich schon zeigt, dass es ist immer schwierig ist durchzusetzen mehr Privacy, weil immer irgendjemand denkt, mit zusätzlichen Daten könnte man irgendwelche Edge Cases vermeiden. Und ich glaube, da ist Verkehrsüberwachung noch vergleichsweise harmlos, weil ich mich da irgendwie im öffentlichen Raum aufhalte und heute schon irgendwie gescannt werde. Ich glaube nicht, dass selbst wenn die Infrastruktur entsprechend ausgerollt wird, werden die Kameras nicht verschwinden. Die haben ja auch noch andere Zwecke. Und insofern bezweifle ich ehrlich gesagt da, dass du mit Privacy irgendwie Überzeugungsarbeit leisten kannst. Das du jetzt in den Kommunen auf einmal jede Ampel noch irgendwie eine kleine Wallet bekommt, also ich glaube, da brauchst du eher monetäre

Anreize, damit da was passiert.

TRANSCRIPT: EXPERT D (GERMAN)

H: Genau. Ich hatte dir ja schon bisschen was zu dem Thema geschrieben, worum es geht. Wenn du möchtest, ich hab ja auch nochmal Folien um das ein bisschen motivieren was ich hier habe. Das ist nichts Besonderes, das sind nur gleich, wenn ich da irgendwie das Framework oder zeige, wenn das notwendig ist. Ja, die Motivation, ich habe es dir ja schon gesagt, ist ein bisschen Verkehrsüberwachung. Wir hatten uns dann nämlich Gedanken gemacht, dass wir einmal einerseits einen Trend sehen, dass die Städte immer digitaler und immer vernetzter werden. Stichwort „Smart City". Wir sehen gleichzeitig, dass dieser Trend zunimmt, dass immer mehr Verkehrsüberwachung eingeführt wird, auf unterschiedliche Art und Weise. Kameras oder dieses Geofencing oder die Übertragung der GPS Position. Und was wir auch gleichzeitig sehen, ist eine Zunahme an Gründen, warum überhaupt eine Überwachung stattfindet. Also in London hast du Umweltzonen, du hast auch diese, diese High Congestion Areas, dass du sagst, in den Innenstädten willst du weniger Autos haben. Und das eben in Kombination mit ja Zahlungen oder Mauten oder das du einfach sagst: Du willst den Verkehr in irgendeiner Art und Weise reglementieren. Das war die Motivation, die wir uns gedacht haben. Ich sehe du grinst schon, du kennst die Thematik?

D: Grundsätzlich, also soll jetzt nicht aus technischer Perspektive, aber es jetzt letztendlich ne Thematik ist, die jetzt im Kommen sein wird beziehungsweise auch schon ist und jetzt gerade natürlich in Verbindung mit IoT wahrscheinlich eine Rolle spielen wird, wenn du entsprechend die Vernetzung hast. Und dann natürlich auch bezüglich der ganzen Thematik. Wenn du dann auch in Richtung autonomes Fahren gehst. Das wird ja dann so ein bisschen die die Schwierigkeiten sein, in denen in der auch sicherlich jetzt aus regulatorischer Sicht noch nicht alles abgedeckt ist, weil da einfach viele Fragen noch offen sind grade bezüglich Haftung beispielsweise.
H: Aber das ist bei dir tatsächlich auch schon Thema, dass du sagst. Ja, das ist etwas, worauf wir, worauf wir achten müssen, auf Landesebene, Bundesebene oder EU-Ebene.
D: Ich würde sagen, es gibt natürlich gewisse Strategien, auch seitens der EU, dass du da beispielsweise gewisse Datenstrategien hast. Das ist jetzt eine Reihe von Verordnungen, die jetzt geplant sind und teilweise auch in Kraft treten, die sich eben allgemein um die Datenstrategie oder mit der Datenstrategie der EU befasst. Und inwieweit jetzt natürlich die ganze Thematik Traffic eine Rolle spielt, kann ich jetzt noch nicht abschließend beurteilen, aber natürlich haben wir auch

da noch ne ganze Reihe auch mit ja nachdem, in welcher Situation KI eine Rolle spielt, da gibt es entsprechend die KI-Verordnung oder einen Vorschlag für eine KI Verordnung, die erstmalig KI überhaupt auf europäischer Ebene regelt und dadurch ist dann eben auch als europäische Verordnung geregelt. Ist dann eben voll harmonisiert und dementsprechend in allen Mitgliedstaaten.
H: Da geht es dann hauptsächlich um die Auswertungen von Daten wahrscheinlich oder?
D: Ich habe es mir neulich en Detail angeschaut, da geht es tatsächlich genau allgemein um, ich sag jetzt mal erstmal der grobe Aufschlag in diese Richtung, in welcher Art und Weise du sowas überhaupt nutzen darfst beziehungsweise in welche Richtung das sich überhaupt entwickelt. Also das ist meines Wissens der erste Ansatz überhaupt, den man in der Hinsicht nutzen kann. Dementsprechend ist das noch alles relativ neu und ist auch nicht direkt hier das Spezialgebiet, mit dem wir uns hier alltäglich befassen.
H: Ja, wobei insgesamt geht das natürlich nahtlos einander über. Also wenn wir uns mit dem Thema Datenschutz befassen oder mit Technologien, die Datenschutz irgendwo ermöglichen. Geht das natürlich schon nahtlos in einander über.
D: Grundsätzlich ja. Allerdings müssen wir natürlich auch hier differenzieren zwischen den Thematiken Datenschutz und Datensicherheit und dann eben auch beim Datenschutz nochmal die Thematik mit, von welchen reden wir überhaupt. Das heißt, personenbezogene Daten sind ja nochmal ganz anders zu bewerten als jetzt letztendlich Maschinendaten. Da ist zum Beispiel dann genau der „Data Act“, wenn ich das richtig im Kopf habe. Das ist eine europäische Verordnung, die sich genau um sich um Datennutzung gerade im Sinne von IoT beispielsweise dreht. Und das sehen wir dann jetzt als Verordnung wie das dann voll harmonisiert in Europa regelt.
H: Also ich mein, wenn ich jetzt zum Beispiel so ein Datenregister habe, dass was wir ja auch, wie wenn dann das Verkehrsministerium die Kennzeichen erfasst oder die deine Verkehrsregister führt, sind das ja dann genau solche Daten, die dann halt auch ausgelesen werden. Wenn du mit deinem Fahrzeug in der Stadt unterwegs bist, du gefilmt wirst. Also das sind dann genau solche Sachen, auch personenbezogene oder eher Maschinendaten?
D: Sowohl als auch. Also die Verkehrsdaten an sich im Sinne von Bewegungsdaten, das sind insoweit Maschinendaten, die haben erstmal keinen Personenbezug, es denn du verbindest das in irgendeiner Art und Weise und könntest entsprechend mehr herauslesen. Ist jetzt bei normalen normales Erachtens nach beim normalen Bewegungsdaten jetzt erstmal nicht unbedingt der Fall. Was anderes ist es natürlich

bei Kennzeichen und eben auch dann, wenn du verbindest, beispielsweise diese Bewegungsdaten mit einem spezifischen Fahrzeug und sagst, du hast in jedem Fahrzeug die, Ich glaub es heißt, FIN, diese Fahrzeugidentifikationsnummer, die auch ein personenbezogenes Datum in dem Sinne darstellt, weil wir mit jeder Nummer entsprechend auf den Halter verweisen kannst.
H: Kannst du mit dem Kennzeichen auch. Das Kennzeichen ist ja auch auf dich zugewiesen als Halter.
D: Genau. Nur bei der FIN hast du zusätzlich noch das Fahrzeug dazu. Also natürlich hast du beim Kennzeichen auch ein Fahrzeug dabei, aber da ist es nochmal ne andere Nummer, weil das Kennzeichen kannst du auch letztendlich mitnehmen. Klar ist es dann auf ein anderes Fahrzeug zugelassen und so weiter, aber die die FIN ist eben einmalig. Die ist nur auf das Fahrzeug selbst zugelassen und kriegt dann erst die Verbindung, indem du letztendlich als Halter das Fahrzeug registrierst. Genau und alles andere, was dann eben Bewegungsdaten anbelangt, das ist dann erstmal IoT oder gerade eben auch welche Daten dann, dass das Auto selbst ausspuckt im Sinne von Nutzungsdaten und ähnliches. Solange es eben nicht direkt Personenzug auf den Halter gegeben ist, wobei man potenziell diskutieren könnte weil das Fahrzeug ja entsprechend registriert ist, dann sind das erstmal IoT-Daten. Und wie gesagt erst ab dem Punkt ab dem der Personenbezug hergestellt werden kann, hast du letztendlich personenbezogenen Daten und dann gehst du in die ganze Zeit DSGVO-Thematik.
H: Wie siehst du das, wenn ich zum Beispiel gerade mit dem Thema Verkehrskamera, die du auf der Straße richtest und dann nicht nur, zum Beispiel das Fahrzeug erfasst, was eigentlich in der Umweltzone einfahren möchte – was ja irgendwo berechtigt ist, dass da diese Kontrolle durchzuführen – sondern zum Beispiel auch Passanten, die vorbeilaufen, Radfahrer die die Straße queren, da bist du ja schon in einem Bereich, wo du sagst, ok da sind Unbeteiligte, in dem Moment, die dann aber trotzdem erfasst werden von dieser Art, von Überwachungsmaßnahme.
D: Ja. Deckt natürlich auch schwer verschiedene oder verschiedenen Perspektiven ab, die man hier betrachten muss. Natürlich ist generell so, dass du, wenn du letztendlich Kameras hast, im öffentlichen Bereich, gerade wenn du als Privatperson oder als juristische Person dann aufstellst, gilt, gleichermaßen die DSGVO. Das heißt, auch da musst du natürlich darauf achten, dass du einerseits entsprechend die Informationspflichten erfüllst. Das heißt, wenn es natürlich leicht dargestellt wird du jetzt sagst, du hast eine Kamera bei einem Gebäude, das du da entsprechend irgendwo ein Schild hast im Sinne von das sind

deine Rechte, so werden diese Aufnahmen verwendet, dann werden sie beispielsweise gelöscht. Das ist jetzt bei einem Gebäude leichter möglich als bei einer Verkehrsüberwachung. Zumal du bei der Verkehrsüberwachung auch nochmal argumentieren könntest, dass du ja hier den ganzen Bereich hast, so dass du hier letztendlich eine öffentliche Aufgabe hast, die erfüllt werden muss. Nämlich genau diese Verkehrsüberwachung. In welchem Umfang das jetzt Zu erfolgen hat, lässt sich streiten. Aber da muss man eben differenzieren zwischen möchte ich jetzt quasi aktiv Verkehrsüberwachung machen oder überwache ich im gesamten Bereich, dann wäre da schon wieder die Frage, was ist da letztendlich die rechtliche Grundlage die du dafür nutzen kannst. Also natürlich kannst du auch in der Öffentlichkeit Kameras nutzen um dann eben zu sagen: „OK, aus Sicherheitsgründen überwachst du eben diesen Bereich“ auch wieder die Frage, welchen Bereich in welchem Umfang, wie wird da gelöscht, weil da nicht nur die DSGVO hast, sondern du auch die ganze Thematik mit Persönlichkeitsrechten, die auch allgemein geltend für jede Person vorhanden sind oder gelten. Das heißt, da hast du dann auch letztlich, die Situation, bis zu welchem Grad kannst du das machen und ab wann ist es dann eben ein Eingriff. Wenn man natürlich dann sagt, wenn du dich als Person in die Öffentlichkeit begibst, ist es natürlich noch etwas anderes, weil du dann letztendlich damit rechnen kannst, von irgendwelchen Kameras aufgenommen zu werden. Man muss da differenzieren zwischen wer genau betreibt beispielsweise das ganze und mit welcher regulatorischen, rechtlichen Grundlage wird das ganze dann gemacht. Das ist eben bei einer Firma, sag ich jetzt mal, leichter herzustellen und zu beurteilen, weil du dann sagen kannst „OK, du beobachtest nur den Eingang“ zum Beispiel, aber auch da ist es so, du darfst den Eingang nur so beobachten, dass du eigentlich nicht den Verkehr oder die Menschen, die vor dem Eingang vorbeilaufen nicht erfasst werden.

H: Die, die unbeteiligt sind.

D: Genau! Da kann man sich natürlich wieder streiten, ab wann bist du beteiligt und wann nicht. Aber das muss man entsprechend auf Feinheiten achten. Und Verkehrsüberwachung? Ja, sag mal, wenn jetzt wirklich nur der Verkehr überwacht wird in dem Sinne, dann hast du ja eine Rechtsgrundlage letztendlich dafür. Dann ist es ja auch irgendwo nachvollziehbar, weil du ja letztendlich auch hier Gefahrenabwehr beispielsweise betreiben willst oder zumindest hier sagst: du hast die Situation, beispielsweise wenn du jetzt Autobahn überwachst, dass du da entweder sagst, du misst beispielsweise Stauaufkommen und Ähnliches und möchtest damit langfristig potenziell gefahren oder Ähnliches vermeiden. Oder natürlich kann man auch gewissen

Sachen sagen, wenn du Richtung und sowas denkst.
H: Ja, oder Anwohnergebiete, dass du sagst, du willst die Anwohner schützen vor zu viel Verkehr. Also ja es gibt schon verschiedene Argumentationen.
D: Wobei die Frage ist, warum überwachst du dann Verkehr?
H: Na gut, das wird tatsächlich, in London zum Beispiel gemacht, dass du sagst, du möchtest nicht, dass die Leute mit ihren Trucks dauerhaft durch die Anwohnergebiete fahren, um eine Abkürzung zu nutzen. Also wie du schon sagst, dass ist bestimmt irgendwo eine Abwägungssache und ob das höhere Ziel dann insofern das Rechtfertig.
Aber da ist natürlich auch die Frage: Das ist ja an sich erstmal kein Freifahrtschein, dass du grundsätzlich mit jeder Begründung dann erstmal die Überwachung einführen kannst oder nicht mit jedem Mittel. Also ist die Frage, gibt es Bedarf an Technologien oder Methoden die da eine gewisse Datensparsamkeit bringen oder erhöhen könnten. Wenn du sagst, ich könnte vielleicht auf eine Kamera verzichten, indem ich eine andere Technologie nutze, die Datensparsamer ist. Und da ist eben die Frage: Gibt es da Bedarf oder gibt es da überhaupt die Notwendigkeit, aber ist eine Nutzung gegeben? Ich glaube, das ist die wichtigste Frage.
D: Gefährlich wird es in der Hinsicht auch, wenn du eben nicht nur die reine Überwachung nimmst, sondern tatsächlich die Auswertung dazu nimmst. Weil letztendlich die Verarbeitung von Daten, ist ja der Gesamtprozess und dann sagst du nutzt daher noch die ganze Auswertung in der Hinsicht dazu, dass du sagst, du machst Themen wie Gesichtserkennung im öffentlichen Raum. Dann reden wir noch ja von ganz anderen gefährlichen Situationen oder potenziell gefährlichen Situationen. Für die Privatsphäre, weil dadurch dann letztendlich Bewegungsmuster erstellen kannst. Du kannst auch da natürlich noch mehr herausfinden. Letztendlich, was dann potenziell Interessen oder Ähnliches anbelangt oder dann eben auch, wenn du das dann natürlich verbindest, noch mit anderen Daten Pools. Dann hast du natürlich ne komplette gläserne Situation, wie es jetzt beispielsweise in China ist. Das wenn du ja dann irgendwie bei rot über die Ampel gehst, wird direkt die Strafe von deinem „Wechat" Konto abgebucht. Das gilt es natürlich auf staatlicher Ebene zu vermeiden, damit du hier keinen Überwachungsapparat hast.
H: Meinst du da ist überhaupt Motivation da von staatlicher Seite für solche Technologien oder ist da eher die die Stimmung: „Je mehr Überwachung desto besser"?
D: Ne klare Tendenz ist das schwierig zu sagen. Ich weiß auf jeden Fall, dass die Situation ist, dass hier beispielsweise durchaus Inter-

esse besteht an Unternehmen wie „Palantir“ zum Beispiel, dass gerade die Polizeibehörden da natürlich Interesse haben eine bessere Vernetzung hinzukriegen. Da natürlich dann auch genau diese Dienste nutzen, um eben diese Erkennung dann auch zu ermöglichen und vor allem auch die Verarbeitung. Dennoch denke ich, dass es bei uns noch relativ entspannt ist, weil ich glaub in anderen Ländern wird das einfach gemacht. Bei uns hast du natürlich regulatorische Grundlagen. Da muss erstmal eine Abwägung stattfinden um dann erstmal festzuhalten, ob wir das überhaupt machen können. Das heißt ich denke das Interesse ist durchaus da, aber kann nicht einfach in der Hinsicht umgesetzt werden, weil wir einfach zu viele regulatorische Sicherheiten haben...

H: Es scheitert an der Bürokratie und an den Regularien!

D: ... genau wir haben zum Glück genügend Regularien, die das Ganze verhindern, damit wir nicht eine Riesen Überwachung haben. Und deswegen beschränkt sich, glaube ich auch, primär ein bisschen die Kameraüberwachung wirklich auf entweder Firmen, das die das Firmengelände überwachen oder Privatgelände, was dahingehend grundsätzlich mit entsprechenden Maßgaben auch zulässig ist. Und ich glaube im öffentlichen Sektor beschränkt sich das wirklich auf Gefahrenbereiche oder eben dann Bereiche, die in der Vergangenheit mal negativ aufgefallen sind. Auch da brauchst du natürlich die entsprechende Begründung, die dann eben erst durch beispielsweise die Historie gegeben sein muss.

H: Das ist auf jeden Fall ein interessanter Punkt, den du da sagst? Ich hab ja schon erwähnt, das Ziel der Arbeit Bayern so ein kleinen Framework – das ist gar nicht wichtig, was da jetzt im technischen Detail überhaupt losgeht. Du kennst das grundsätzliche SSI-Schema ja. Du hast Aussteller, du hast Holder und du hast am Ende halt den Verifier. Die Grundidee von dem Framework ist einfach, du setzt im Prinzip im öffentlichen Raum integriert in deinen Smart City Kontext, sag ich jetzt, auf verteilte Verifier, mit denen du dann mit deinem Fahrzeug kommuniziert und darüber Credentials austauscht. Das ist die Grundidee, die Credentials kriegst du quasi als Fahrzeughalter ausgestellt, überträgst sie an dein Vehicle und das Vehicle führt dann praktisch auf den Proofrequest die Präsentation aus.

D: In welchem Gesamtkontext läuft das Framework? Ist es quasi jetzt bezogen auf Städte oder dann spezifisch auf gewisse, ich sag jetzt mal kleinere Orte.

H: Es sind praktisch kleinere Areale innerhalb einer Stadt. Eines der Beispiele, die ich häufig anführe, ist eben das Thema Anwohnerviertel, dass du sagst du brauchst einen Parkausweis um reinzufahren oder Anwohnerausweis. Den würdest du dir praktisch von einem

Meldeamt ausstellen lassen, legst es in deinem Auto ab, als Pool, als Sammelstelle für deine Credentials und dann wird Zero-Knowledge Proof gefragt, darfst du überhaupt rein. Dahingehend ist das praktisch nur für kleinere Stadtareale gedacht.
D: Also wo erfolgt die Prüfung per Schranke, dann irgendwo am Anfang oder?
H: Die Prüfung an sich erfolgt erstmal innerhalb ja der normale Infrastruktur, das kann eine Straßenlaterne sein oder eine Ampel. Interessant ist die Frage was passiert wenn du keine Berechtigung hast um einzufahren, dann musst dann im Prinzip eine entsprechende Logik dahinter liegen, die dann sagt „du hast ja keine Berechtigung". Dann kann es natürlich passieren, dass dann nochmal auch das Ordnungsamt mal geschickt wird um das zu kontrollieren.
D: Wird sicherlich dann auch in der Hinsicht die Frage sein, in wie weit man darauf beschränken. Weil du hast natürlich irgendwo dann die Situation, dass du was beschränken darfst, aber es darf natürlich dann nicht irgendwie zu extrem sein, dass man auf einmal sagst. OK, du hast komplett voll vernetztes Auto und dann mit dir dadurch quasi per Fernzugriff das Auto abgestellt.
H: Ne, das ist das tatsächlich nicht die Sache. Es soll auch explizit so sein, dass keine personenbezogenen oder fahrzeuginternen Daten mit übertragen werden, sondern am Anfang geht es tatsächlich nur darum: Ist es ein Anwohner? Darf er in das Viertel rein oder darf er das theoretisch nicht?
D: Genau, da geht ja mit Zero-Knowledge Proof auf jeden Fall.
H: Eine andere Idee war zum Beispiel, dass du dir von der Krankenkasse eine Art Behindertenausweis ausstellen lässt oder für besondere Beeinträchtigungen, um damit dann auf bestimmte Parkplätze fahren zu dürfen. Ist dann ein ähnliches System was du wahrscheinlich dann über eine Schranke dann lösen könntest.
D: Oder eine Sensorik im Boden. Was es teilweise jetzt gibt, Ich glaube bezüglich der Zeiten, hast du ja auch auf manchen Parkplätzen das dann das Timing getrackt wird. Ja, guter Ansatz.
H: Und das ist eben auch die Frage. Wie so ein Framework ja erstmal von der Draufsicht her zu bewerten ist, ob das machbar ist. Auch von der regulatorischen Seite her. Oder ob man sagen würde, ne, können wir auf keinen Fall machen, das Auto irgendwie einen SSI-Proof durchführt. Ob da irgendwie was dagegen spricht? Das könnte ich jetzt so im ersten Moment nicht sagen.
D: Genau. Du hast bei der Regulatorik auf jeden Fall, auch wenn natürlich IoT immer noch so ein bisschen auch in der Diskussion ist, inwieweit das ganze IoT erweitert wird. Wir haben aber natürlich bei der Regulatorik, gerade jetzt in dem Vorschlag beziehungsweise

in den nächsten Jahren. die ganze Thematik mit der eiDAS2. Und hier haben wir natürlich dann erstmals die Situation, dass wir hier gleich zur eiDAS 1, ich sag mal erstmalig, die Situation haben, dass wir überhaupt diese ganze Thematik Verifiable Credentials in irgendeiner Art und Weise auch geartetes rechtliches Konstrukt kippen können. Das heißt, wir haben hier oder es ist zumindest geplant, dass wir sogenannte Qualified Electronic Attestations of Attributes haben, was letztendlich nichts anderes sind als verfiable Credentials, nur eben dann mit dem entsprechenden rechtlichen Konstrukt. Das sind eben Attribute, die eben ausgegeben werden von beispielsweise Vertrauensdienste-Anbietern die wiederum, jetzt als zertifizierte Dritte natürlich gewisse Auflagen erfüllen müssen, wobei man auch da natürlich noch streiten kann oder argumentieren kann, dass man hier differenzieren zwischen den Qualified Electronic Attestations of Attributes, die ihm dann nur von qualifizierten Vertrauensdienste-Anbietern ausgegeben werden dürfen, die wiederum gewisse Auflagen erfüllen müssen. Oder du hast eben die Situation, dass quasi normale Vertrauensdienste-Anbieter, die nicht diese strengen Auflagen erfüllen müssen, keine qualified credentials ausstellen können, sondern quasi normale Attributes. Natürlich, und da muss man differenzieren, je nachdem, wieviel Vertrauen muss an dieses Attribut gestellt werden, dass man sagt ok ein digitaler Führerschein braucht natürlich weitaus höheres Vertrauen als irgendein Mitgliedsausweis, den du jetzt bei deinem Fitnessstudio bekommst. Weil du natürlich sagen kannst: ok mit dem kannst du jetzt nicht so viel anfangen. Da ist keine Gefahr gegeben. Genauso hättest du den auch hier die Situation, dass du natürlich differenzieren müsstest zwischen diesen Attributen, die ich jetzt hier ausstelle. Wenn man jetzt sagt ok Berechtigungsscheine entsprechend für Anwohner scheinen jetzt schon wieder ein Stück weit was offizielleres, weil du ja dann das eben nur von der Stadt kriegst, kann also dann durchaus wieder höhere Auflagen haben als eben gleich jetzt ne Mitgliedskarte. Zumal du ja hier auch dann gegen öffentliche Register das Ganze beispielsweise prüfen musst, ob das überhaupt gegeben ist. Das heißt, auch da brauchst du überhaupt wieder die Schnittstellen und die Zugänge, die wiederum ja auch nur die Behörden haben.

H: Dann reden wir in der Praxis dann auch tatsächlich von kryptographischer Sicherheit, um sowas dann auszustellen.

D: Genau und da ist ja es auch gut so, dass da nicht jeder darauf Zugriff hat. Das man jetzt direkt dann prüfen kann, welche Personen jetzt an welcher Stelle wohnt, an welchem Ort wohnt. Aber das ist zumindest jetzt langfristig denkbar. Das heißt, wenn wir jetzt auf jeden Fall die Situation haben und das wird voraussichtlich dieses Jahr zu-

mindest erstmal fertig verhandelt. Und dann erstmals das ein fertiger Vorschlag überhaupt verabschiedet wird. Kann durchaus noch dieses Jahr erfolgen. Spätestens Frühjahr nächsten Jahres. Und dann hast du die Übergangsfrist von 2 Jahren, also eine entsprechende Umsetzungsfrist. Und parallel werden ja auch entsprechend die ganzen Wallets, die dann natürlich auch eine Rolle spielen von den Mitgliedstaaten, also die, die Wallets werden von Mitgliedstaaten herausgegeben, jeweils. Und da wird ja auch aktuell daran gearbeitet, beziehungsweise an entsprechenden Pilotverfahren wird gearbeitet, wie man das umsetzen kann. Das heißt, auch da ist dann die Situation, dass du später das Ganze natürlich bequem in einer Wallet machen kannst. Da ich dann eben meine eID beispielsweise verbunden habe oder gemeinsam in diesem Wallet integriert habe inklusive eben dieser Attribute. Und dann zum Beispiel auch gar nicht mehr ins Amt gehen muss, sondern einfach sagen kann, wenn ich jetzt meine eID nehme und dann einen Request an das Amt schicke, dass ich da das entsprechende Credential ausgestellt bekomme. Ich kann dann quasi nachprüfen, ich bin ich und ich wohne hier und dann bekomme ich eben dieses zusätzliches Attribut ausgestellt, diese zusätzliche Credential für eben genau diese Verfahren. Und das ist jetzt zumindest mal überhaupt denkbar, dass man da nicht mehr jetzt irgendwelche Aspekte um die Ecke denken muss, sondern wenn das alles so läuft oder umgesetzt wird, wie es jetzt aktuell in dem Vorschlag vorgesehen wird. Dann besteht eine gute Chance, dass man diese ganze Technik, die jetzt dahinter steht oder auch die Technik hinter SSI steht auch überhaupt mal regulatorisch absichern kann.

H: Das heißt, du siehst ja auch schon, am Horizont sozusagen, für die Technologie, da auch Potenzial, dass das ausgerollt wird?

D: Ja! Man muss natürlich sagen oder man muss differenzieren, dass man jetzt überlegt, wieviel SSI wird da wirklich drin stecken. Weil du hast natürlich immer nur einen gewisse Grad an Kontrolle, den du im Kontext einer hoheitlichen ID ausüben kannst. Man muss immer auch differieren zwischen dass man ja sowohl eine digitale Identität haben kann, aber das muss nicht immer gleich sein mit der hoheitlichen Identität. Wenn du jetzt allerdings hier von diesen offiziellen Prozessen sprichst, wie jetzt hier im Framework auch verankert sind, das wird höchstwahrscheinlich über die hoheitliche ID auch ablaufen.

H: So war auch der Hintergedanke, ja.

D: Ja, genau. Und da hast du natürlich auch entsprechend die offiziellen Credentials. Und da hast du dann natürlich immer einen Gewissen eingegrenzteren Spielraum im Vergleich zum gesamt SSI-Gedanken, weil du dich da ja genau an die Regulatorik halten musst.

Und da es ja gewisse Auflagen gibt, wie du auch mit deiner ID umzugehen hast. Und da ist ja dann auch diese ganze semantik Zero-Knowledge Proof aktuell noch nicht drin verankert. Das heißt das wäre natürlich vorteilhaft, weil das natürlich auch den ganzen Datenschutz mit sich bringt. Das heißt, wir haben grundsätzlich natürlich immer wieder den Verweis auf den Datenschutz, die Grundprinzipien mit Datenminimierung, Datensparsamkeit und Co. Aber mit Zero-Knowledge Proof hättest natürlich erstmalig auch die Möglichkeit das wirklich technisch umzusetzen.
H: Ja ist ein guter Punkt, den du da sagst. Weil Kern von den Zielen, die das Framework auch verfolgt ist nämlich tatsächlich auch wie du schon sagst, das Thema Datenminimierung. Das wir nämlich auch tatsächlich sagen können, es gibt eine Möglichkeit, den Verkehr insofern zu regeln oder ein Identitätsmanagement einzuführen, ohne dass du halt permanent deine Umgebung überwachen musst. Sondern dass es dann wirklich zwischen Infrastruktur und Fahrzeug dann praktisch diese Kommunikation aufgebaut wird und dieser Austausch erfolgt. Gleichzeitig hast du auch nicht diese Gefahr, dass dann auch Bewegungsprofile erstellt werden müssen, weil du andauernd deine Position in irgendeiner Art und Weise versendest. Und dahinter gelagert ist dann tatsächlich so Gedanke, dass du auch so n bisschen deine, Credentials oder deine Attribute, die du als Person hast, auch so ein bisschen von deinem Fahrzeug tatsächlich auch kannst. Das Thema FIN hatten wir gesagt, dass er irgendwann im Zentralregister liegt oder dein Kennzeichen was registriert ist. Und dadurch, dass du dann praktisch sagst. Ich halte praktisch meine Attribute in meinem Wallet und ich halte die Fahrzeugeattribute in einem Fahrzeug-Wallet und dadurch kannst du dann tatsächlich sagen, da findet noch ein bisschen etwas stärkere Trennung statt als es jetzt aktuell irgendwelchen Zentralregistern ist.
D: Das sowieso. Also das sollte sowieso nicht irgendwie in Zentralregistern landen, weil wir dann sowieso irgendwann eine noch stärkere Überwachung haben gerade bezüglich der Bewegungsprofile, die ja derzeit zum Glück nirgendwo bisher gespeichert werden. Das heißt, da muss man jetzt natürlich diskutieren. Weil du kannst, selbst wenn du es jetzt technisch trennst zwischen Fahrzeug- und Personen-Wallet, letztendlich nie eine vollständige Trennung haben. Weil natürlich kannst du in dem Moment nicht unbedingt nachvollziehen, wer fährt. Außer du sagst immer, ok du verbindet dich eben dann in dem Moment auch, was natürlich vielleicht auch irgendwo Vorteile haben kann. Das du dann sagst, du hast gewisse Datensätze, die du nur auf dem Auto speicherst, die ich als Fahrer dann brauche. Zur Not. Fällt mir jetzt ad hoc nichts was da jetzt gut passen würde, aber.

H: Ja, vielleicht tatsächlich so Emissionswerte oder sowas. Wenn du sagst Komponenten für eine Umweltzone, was halt reine Fahrzeugattribute sind. Das ist tatsächlich sowas, das du nur auf dem Fahrzeug liegen lassen würdest.
D: Genau die, das sind Fragen, warum ich als Fahrer jetzt diese Daten bräuchte.
H: Ja, maximal um die irgendwo vorzuzeigen.
D: Genau, wann zeigst du diesen denn vor?
H: Wenn dann würde das Fahrzeug das wahrscheinlich dann selber auch wieder in so einem Kontext vorzeigen.
D: Genau. Also da muss man natürlich dann schauen, wie man da differenziert. Aber grundsätzlich ja. Also das sind natürlich denkbare Differenzierungen, die man da vornehmen kann. Jetzt musst du mir nochmal kurz auf die Sprünge helfen? War die die Grundfrage hinter dem?
H: Ja, die Grundfrage, ob das so am Ende des Tages umsetzbar ist. Das du sagst, du erreichst diese. diese Trennung von Identitäten und auch das Vermeiden von eben diesen Überwachungsmechaniken
D: Genau also ich denke, grundsätzlich wirst du es nicht vermeiden können. Dadurch, dass das Fahrzeug eben durch diese Nummern personenbezogenen Daten beinhaltet und dementsprechend Personen beziehbar ist. Wirst du, auch wenn es nicht direkt erkennbar ist, wird es zumindest über Umwege ermöglicht. Das heißt, es sind keine direkten personenbezogenen Daten, die du hast, aber sie sind Personenbeziehbar. Das heißt, gewisse Dritte haben die Möglichkeit, eben durch Abfrage in Registern nachzuweisen, wem dieses Fahrzeug gehört und dadurch hättest du wiederum die Verbindung. Also eine komplette Trennung, in der Hinsicht sehe ich nicht, es sei denn du hast wirklich die Situation, dass du autonome Fahrzeuge hast, die eben in der Flotte beispielsweise fahren. Dann glaube ich, hast du wirklich die Situation, dass du reine IoT-Daten hast, die sich nur auf das Fahrzeug beziehen, weil dann bei wechselhaften Personen hast vielleicht ne Firma, die hinter dieser Flotte steht, diese Flotte registriert hat, aber du hast keine Einzelpersonen mehr.
H: Ich meine, das wäre natürlich auch in ferner Zukunft vielleicht irgendwo ein Use Case, dass du gar kein eigenes Fahrzeug mehr hast, sondern über Carsharing oder über Dienste dann hingehst und nicht mit einem Auto verbindest. Vielleicht sogar mit deiner Wallet dann verknüpfst.
D: Genau da hast du genau da wieder die Verbindung, weil ich ja dann sagen kann, OK, ich würde mich gegenüber dem Fahrzeug ausweisen wer ich bin und würde mit dem Fahrzeug quasi entsprechenden Proof schicken, dass ich eben beispielsweise im Besitz eines gülti-

gen Führerschein bin. Und damit hätte ich wieder die Verbindung.
H: Das ist aber auch die Frage, ob das für das Fahrzeug ausreichend ist oder ob das Fahrzeug dann nochmal an einen Server irgendwo schicken muss und das dann speichern muss um da diese Abfrage zu machen.
D: Vermutlich, aus Haftungsfragen, an irgendeiner Stelle ja.
H: Ok das ist dann Die Haftungsregulatorik.
D: Ja. Natürlich könnt ich dann mit Zero-Knowledge Proof prüfen: Hast du einen gültigen Führerschein – ja / nein – ok schön und gut, aber spätestens wenn irgendwas passiert, muss ich ja irgendwie dann gerade bezüglich der Versicherung oder ähnliches brauch auch dann die Nachweisbarkeit und auch da wird ja auch bei der Buchung zum Beispiel wahrscheinlich irgendwas an Daten anfallen, die wiederum auf den spezifischen Fahrer zurückzuführen ist. Das heißt, wahrscheinlich wirst du immer irgendwo diese Verbindung haben. Ich sag mal so, auch da wird es noch Diskussionen geben, wie das bei autonomen Fahrzeugen überhaupt ist, weil da ist natürlich überhaupt die Frage mit Haftung, wenn ein Unfall passiert, hafte ich als Beifahrer oder. . .
H: . . . oder der Hersteller.
D: Also wenn ich hinten sitze und quasi keine Möglichkeit überhaupt zu agieren. Das heißt, wenn ich als reiner Beifahrer. Ist halt die Frage, ob für mich diese Haftung überhaupt relevant ist. Die Haftung ist für mich relevant, wenn es zu Personenschäden in meiner Person kommt, dann ja, weil da hab ich Interesse dran, aber gegenüber dem Fahrzeug kann man durchaus argumentieren oder sich auch überlegen, dass ich als reiner Mitfahrer da gar nichts mit tun habe. Wenn ich wirklich null Einflussmöglichkeiten habe auf das autonome Fahren. Was dann natürlich auch wieder davon abhängt, von welchen verschiedenen Schritten wir bei dieser Autonomie reden. Beim autonomen Fahren.
H: Ja, das ist wird aber noch sehr Zukunftsmusik.
D: Genau das ist noch Zukunftsmusik, aber das sind diese Haftungsfragen, die Juristen jetzt schon beschäftigen, die dann immer noch Frage sein wird, wie. Genau wie „Wer haftet dann?“.
H: Ja, auf jeden Fall sind das auch alles Punkte, wie du schon sagst. Haftungsfragen habe ich so wahrscheinlich nicht richtig bedacht, aber ist auf jeden Fall wichtig, dass auch irgendwie mit einzubeziehen oder zumindest zu sagen da ist noch was auf der rechtlichen Seite das da zu beachten ist. Ja ist interessant also, da könnten wir wahrscheinlich noch Stunden drüber diskutieren, aber ich glaube du musst auch wieder arbeiten. Hast mir auf jeden Fall schon weitergeholfen.
D: Gerne, gerne.
H: Einfach nur aus der Sichtweise, dass des Juristen drauf zu schauen,

ist auf jeden Fall interessant. Hast du noch irgendwelche Fragen oder ist irgendwas unklar?
D: Nicht direkt also das Gesamt-Framework würde mich natürlich noch interessieren, weil du gesagt hast das jetzt bezüglich auf einzelne Arealen in der Stadt, ob es noch ein übergreifendes Netzwerk dann gibt, was dann da auch eben nochmal ne Rolle spielt oder ob es tatsächlich dann angebunden ist an die Behörde vor Ort. Das da eben noch der Knotenpunkt ist oder wie ja spielen diese Areale zusammen? Ist das noch so ne Thematik?
H: Dahingehend, dass du sagst oder weil du eigentlich sagst, es gibt verschiedene Gründe, solche Areale mit Restriktionen zu versehen, besteht da eigentlich erstmal keine Kopplung oder kein Zusammenhang. Also wenn ich als Stadt zum Beispiel sage, ich hab ein Areal für Anwohner, ein Areal als Umweltzone, die könnten sich theoretisch überlappen, die könnten aber auch komplett disjunkt sein. Das ist erstmal dezentral organisiert und wahrscheinlich von Kommune zu Kommune unterschiedlich. Was in der Hinsicht dann halt mehr oder weniger zentral oder ja, geordnet passiert, ist eben dieses Thema Ausstellung. Das du sagst, es gibt eine Liste an Ausstellern für solche Eigenschaften und das was dann eben ausgestellt wird, das wird dann entsprechend geprüft, wenn du so ein Areal betrittst. Aber das ist auch ein bisschen der Hintergedanke, dass du wirklich versuchst, so etwas entkoppelt zu bekommen und dass das nicht alles hierarchisch von oben nach unten drunter diktiert wird. Und ja, das ist so ein bisschen noch ein theoretisches Gespinst. Das ist alles noch nicht. 100%ig durchdacht aber da wird es noch viele, viele Iterationen durch geben. Aber ja, ich bin mal gespannt, ob das Anklang findet. So eine Idee oder so ein Konzept.
D: Ja, also ich sag mal so die die Perspektive ist ja gegeben. Und sowohl bezüglich der ganzen Thematik Identity als auch in Bezug auf IoT und autonomem Fahren. Das ist sicherlich eine Thematik, auch wenn man natürlich mit entsprechendem Fingerspitzengefühl rangehen muss, wo quasi die Grenze ist und mit dem, was du darfst und in wie weit darf da eine Kommunikation zwischen beispielsweise Fahrzeug und Umgebung stattfinden. Das wird sicherlich kommen, also sowohl dass man sagt, es ist positiv, dass auch dem Verbraucher dann im Endeffekt hilft, als auch, dass es dann natürlich auch dystopisch skizzieren könnte, dass man dann eine totale Überwachung hat.
H: Deswegen finde ich es eigentlich auch wichtig sich mit solchen Themen frühzeitig zu beschäftigen, bevor es eigentlich schon Standard geworden ist. Das man dann auch wirklich sagen kann, wir haben uns schon Gedanken gemacht, egal wie gut oder wie schlecht die Frameworks am Ende werden. Aber man kann zumindest als Aus-

gangspunkt benutzen für weitere Arbeit. Ja, wie gesagt, vielen Dank, dass du dir die Zeit genommen hast.
D: Sehr gerne.

TRANSCRIPT: EXPERT E (GERMAN)

H: Wenn du trotzdem noch mal so nett wärst und kurz sagen, was dein wissenschaftlicher Hintergrund ist und wie lange du dich so mit deinem Schwerpunktthema beschäftigst, das wär super.
E: Genau. Also mein Name ist [REDACTED]. Ich bin wissenschaftlicher Mitarbeiter bei Professor [REDACTED] und wie man hier im Hintergrund sieht, eben am Forschungsinstitut [REDACTED] und dem [REDACTED]. Und genau, wir sind ein ja standortübergreifenden Forschungsinstitut im Bereich Information Systems und ja IT Organisation. Da bin ich Doktorand, seit jetzt fast einem Jahr und hab doch davor an der Universität [REDACTED] Bachelor und Master studiert. Tatsächlich noch Betriebswirtschaft. Im Master dann, da das sehr modular aufgebaut ist an der Uni [REDACTED] mit hauptsächlich Wirtschaftsinformatikmodulen. Und die Promotion jetzt eben auch in Wirtschaftsinformatik. Und genau wie komme ich zu SSI oder was ist mein SSI Bezug? Ich habe tatsächlich auch meine Masterarbeit schon über SSI geschrieben. Also grundsätzlich von meinem Hintergrund her: Ich komme ein bisschen aus der Operations Management-Schiene her, das heißt so Supply Chain Management, Beschaffung, Einkauf, Lieferketten, Nachvollziehbarkeit - jetzt insbesondere eben durch SSI auch. Und dann war das tatsächlich meine Masterarbeit. Und das vielleicht auch noch aus dem Forschungsbereich, komme ich grundsätzlich eher so aus dem aus der Ecke „Blockchain“. Da habe ich meine Bachelorarbeit schon über Blockchain im Einkauf geschrieben, um mit der Masterarbeit hat sich das Ganze dann noch konkretisiert auf SSI für Interorganisationaler Informationsaustausch. In der Domäne also immer unter der Linse des Supply Chain Optimierung, aber eben auch in Richtung Lieferketten, Nachvollziehbarkeit. Seitdem bin ich auch in der „SSI Sphere“ unterwegs. Ansonsten bin ich innerhalb des [REDACTED], also unseres Forschungsinstituts, haben wir ein Blockchain-Labor. Auch von [REDACTED]. Dort bin ich Mitglied. Und ja, wie dieser generelle Shift von Blockchain, vielleicht mit relativer Krypto- beziehungsweise Währungsdomäne sich immer weiter zu neuen Use Cases entwickelt hat, haben wir dort auch im Lab einen Shift insbesondere zu sicheren digitalen Identitäten und erforschen dort alle möglichen Bereiche. SSI zum Beispiel. Auch noch deutlich technischere Themen wie Zero-Knowledge Proofs oder wie man einfach grundsätzlich irgendwie Daten, die nicht unbedingt auf eine Blockchain sollten, trotzdem durch diese verifizierbar machen oder sicher hinterlegen kann, und lauter solche Sachen.
H: Ja, ist auf jeden Fall. Interessant was du da beschreibst. Wie lange bist du denn ungefähr jetzt so im SSI-Thema aktiv? Du hast hat schon

Erfahrung.
E: Das war noch in meinem Master, das heißt seit 2020/2021... Ende 2020 würde ich sagen, ja. Hat das angefangen. War tatsächlich dort zu der Zeit auch das neue Paradigma, was gerade aufkam, wo man sich eben umgeschaut hat. Diese Technologieagnostik, die man ja irgendwie Blockchain nicht hat, sondern genau umgekehrt - man hat irgendwie diese Technologie gehabt und auf einmal hat Use Cases gesucht - und dann kam das so langsam auf, dass man überlegt hat, „ah Identitäten könnten irgendwie ein neuer Blockchain Use Case sein". Dann kam diese „Principle of Alan" auf, die relativ abstrahiert man dann aber auf diese Blockchain-Funktionalitäten gemappt hat und dann gesehen hat, „Ah das könnte für uns auch spannend sein im [REDACTED]". Also, so zweieinhalb Jahre würde ich sagen.
H: Oh cool. Ich teile mal kurz meinen Bildschirm. Siehst du meine Folien?
E: Ja.
H: Ah, perfekt. Ich würde kurz ein bisschen auf die Ausgangssituation eingehen, die wir uns so gedacht hatten in dem Forschungsfeld. Ein bisschen auf das Framework eingehen, was wir uns ausgedacht haben, beziehungsweise dann nochmal auf die Design Objectives, die dann durch das Framework erfüllt sein sollen.
Tatsächlich, unsere Ausgangssituation beschäftigt sich mit einer Smart City-Situation. Weil wir sehen: Heutzutage geht der Trend immer mehr zu vernetzten Fahrzeugen, zu vernetzter Infrastruktur. Gleichzeitig sehen wir aber auch eine Steigerung von Verkehrsüberwachung, was ein sehr großer Punkt ist. Wir sehen hier ein bisschen in den Folien, das ist hauptsächlich mit Kameras und Nummernschild-Erkennung. Das ist aber auch ganz oft mit ja individuellem SIM-Tracking oder dass das Fahrzeug selber seine GPS-Koordinaten überträgt. Und was wir als drittes auch noch festgestellt haben ist, dass immer mehr Gründe existieren, um auch Fahrzeuge zu überwachen. Also das sieht man ganz gut in Städten wie London oder auch Paris. Es werden immer mehr Sonderzonen innerhalb von Stadtarealen errichtet. Seien es jetzt Umwelt-Hintergründe oder seien das Maut-Hintergründe oder einfach, weil man sagt man möchte Anwohner schützen, vor zu viel Verkehrsbelastung. Und das sind immer wieder neue Gründe, warum sich die Städte überlegen. „OK, hier führen wir ein Monitoring ein und hier haben wir dann tatsächlich auch die Technologien dafür".
Ganz oft eben mit dem Nachteil von Datenschutz und eben dem Profiling von Fahrzeugen. Oder zum Beispiel bei Verkehrskameras, die dann eben auch nicht nur die eigentlichen Fahrzeuge aufnehmen, sondern zum Beispiel auch Passanten oder Fahrradfahrer oder Leute, die gar nicht in das Stadtareal einfahren möchten. Was wir uns jetzt dazu

gedacht haben: OK, vielleicht kann man das besser lösen, indem man zum Beispiel sagt, man geht in die Richtung dezentrale Identitätsverwaltung.
Dazu haben wir uns ein kleines Framework überlegt. Das fängt relativ einfach an und sagt, wir haben öffentliche Einrichtungen, die einem zum Beispiel einen Anwohnerparkausweis ausstellen können, wie Meldeämter es jetzt auch schon tun. Oder Krankenkassen, die einem zum Beispiel Bescheinigungen ausstellen können, für Menschen mit Beeinträchtigungen, dass sie in besondere Areale einfahren oder parken dürfen. Und diese Form von Bescheinigungen bekommt man dann als Verifiable Credential ausgestellt. Kann sie über eine App, oder wie auch immer man das verwalten möchte, dann in seinem eigenen Wallet auch hinterlegen. Und das Ganze ist natürlich auch verankert in einer Form von Vertrauensanker. Das ist das was ganz oft Blockchain ist im klassischen SSI Kontext muss es aber auch nicht sein. Es gibt ja verschiedene Möglichkeiten wie man das hinterlegen kann. Was jetzt dazu kommt, ist praktisch - ein bisschen gespiegelt - , dass wir jetzt auch das Fahrzeug mit einem Identity Wallet ausstatten wollen. Da können wir schon gleich sagen: OK. Wenn das Fahrzeug vom Hersteller vom Band läuft, kann es zum Beispiel schon ein Verifiable Credential ausgestellt bekommen über gewisse Fahrzeugeigenschaft. Zum Beispiel, für Umweltzonen relevant, was so die die Komponenten ja mitbringen, um eventuell in der Umweltzone einfahren zu dürfen oder nicht.
Was jetzt wahrscheinlich neu dazu kommt, ist die Möglichkeit, dass der Fahrzeughalter seine ausgestellten Credentials per Delegation, oder welche Technologie auch immer, mit an das Fahrzeug übertragen kann. Das heißt das Fahrzeug wird zu einem Pool, zu einem ja Sammelbecken für die verschiedensten Formen von ausgestellten Credentials. Und wenn wir dann praktisch in einem Punkt sind, dass der Fahrzeughalter mit dem Fahrzeug unterwegs ist in einem bestimmten Stadtareal eintreffen oder einfahren möchte. Dann passiert dann tatsächlich auch diese Proof-Abfrage und Präsentation von Seiten der integrierten Infrastruktur.
So ist praktisch der einfache Use Case. Wie wir uns das erstmal gedacht haben, das praktisch der einfachste Case. Ist das soweit verständlich, wenn ich dir die Architektur so zeige?
E: Ja, das ist verständlich. Genau. Also ich habe schon eine Frage. Weiss nicht ob ich die jetzt schon stellen soll.
H: Gerne, ja bitte.
E: Also genau, was ich nicht ganz verstehe ist die vom Owner ins Vehicle abgegebenen Credentials. Was wäre das und warum sollte man die im Auto halten?

H: Ja, das ist eine gute Frage. Und zwar ist einer der Hintergründe, dass wir zum Beispiel gesagt haben die Ausstellung von einem Anwohnerausweis. OK, ich wohne jetzt hier, in meinem Fall in [REDACTED]. Ich darf hier in der Innenstadt wohnen und dürfte hier theoretisch auch parken. Und dieser Nachweis wird erstmal mir als Person ausgestellt. Jetzt ist es tatsächlich so. Ich muss mir das physisch ausdrucken, muss es praktisch in meine in meine Windschutzscheibe legen und dann wird es eventuell von ja einem Ordnungsämtler überprüft.
Das ist so der Use Case, dass man sagt, man macht ne technische Lösung daraus. Und sagt, es wird mir zwar weiterhin ausgestellt, kann auch digital jederzeit ausgestellt werden und ich kann das von meinem Wallet auf das Fahrzeug übertragen. Das kann praktisch direkt vom Fahrzeug aus gespeichert und bei Bedarf vorgezeigt werden. Ich kann aber auch zum Beispiel hergehen und sagen: OK, ich hab vielleicht gar kein eigenes Auto, sondern ich miete mir regelmäßig Autos oder ich ja bin gerade mit dem Auto von meiner Partnerin oder meinem Partner unterwegs und denen möchte ich jetzt auch die Möglichkeit geben, in dieses Areal einfahren zu dürfen. Und dann kann zum Beispiel sagen, OK, mein Credential könnte ich jetzt auch mit übergeben. Das wären zum Beispiel solche Use Cases. Das ist schon ein bisschen weiter gedacht, da kommen wir vielleicht später noch drauf, aber das wäre zum Beispiel ein möglicher Use Case.
E: Okay ja, verstehe ich.
H: Grobe Architektur haben wir gesagt, Ok die ist eindeutig. Siehst du da irgendwo etwas woran es hapern könnte oder aus deiner Erfahrung wo da Schwierigkeiten auftreten könnten?
E: Ja genau. Also ich würde tatsächlich sagen, an der Stelle, da ist der große Knackpunkt. Auch wie du eben erklärt hast, in den Beispielen muss man dann ja sehr genau unterscheiden: Ist das jetzt irgendwie ein Credential, was auf eine Person ausgestellt wurde und jetzt nicht zwangsläufig zum Auto gehört, aber dann dort irgendwie in der Wallet liegt. Das heißt, das ist irgendwie wieder im Bereich Revocation. Wie krieg ich denn jetzt aus einem Mietwagen meinen Credential-Zugang zur Innenstadt von [REDACTED] wieder raus? Damit nicht, der Nachmietende nach mir, damit dann da irgendwie reinfährt.
Deswegen hab ich auch diesen Punkt: Warum sollte ich in einem Vehicle-Wallet irgendwas halten, außer man könnte das halt sehr klar trennen, deswegen weiß ich nicht ob Verifiable Crednetial, also in den mittleren Pfeil von Owner zu Vehicle, das Richtige ist oder ob das nicht eigentlich auch ein VP ist also eher eine Präsentation in dem Sinne. Also quasi ein transformiertes und nicht das Credential sein. Das Credential sollte meiner Meinung nach immer in der einen Wal-

let bei User liegen und dann hat der Owner seine Credentials und das Vehicle hat seine Credentials. Aber wenn du jetzt als Owner in Credential auf Vehicle überträgst, dann ist das nicht mehr das Ur-Credential, sondern das müsste ja auf jeden Fall irgendwie vielleicht doch kryptographisch irgendwie transformiert sein. Und das würde ich vielleicht noch kenntlich machen. Also wenn das, wenn ihr das auch so vorabt, weil so 1 zu 1 Credential übertragen, da sehe ich auf jeden Fall Probleme mit der ganzen Thematik Access Management, Revocation, Updates und ähnliches.
H: Ja, also müsste wahrscheinlich durch ne Technologie sein, was ja so gibt Authentic Chained Data Containers oder sowas, müsst das passieren um überhaupt diese Transitivität herstellen zu können. Von Issuer zu Holder und dann zu Vehicle.
E: Genau, ja.
H: Hast du eventuell schon mal Erfahrungen gemacht, wie generell Credentials übertragen werden? Also auf einer technischen Art und Weise? Also welche, welche drahtlos Technologien werden denn zumindest in deinem Kontext hauptsächlich verwendet?
E: Eigentlich soweit ich weiß nur Web-based, tatsächlich. Also wir haben jetzt zum Beispiel irgendwie mit [REDACTED] mal so ein Concept gehabt, das man auch mal durchspielen konnte. Und das wäre dann ja auf jeden Fall Web-based. Den anderen Anwendungsfall, den ich jetzt kenne, ist, dass ich mal mit dieser Ausweis App 2.0 oder so. Da rum experimentiert hab und da wäre es ja quasi über so RFID oder NFC Chip von der Karte aufs Handy zum Beispiel gewesen. Ja, das wäre jetzt die 2 Sachen die mir einfallen aber primär würde ich sagen. Web- oder Internet-based.
H: Ja, für den Hintergrund, dass man praktisch was so sieht, was sind die gängigsten Übertragungstechnologien. Denn auch beim Thema hier, Infrastruktur, auch da ist die Frage, wie man zum Beispiel mit der Infrastruktur kommunizieren könnte. Also das, was heutzutage auch schon verbaut ist, ob man da sagen kann, vielleicht kann man die ja Verkehrsampel oder vielleicht eine Straßenlaterne oder so, ausstatten mit entsprechenden Technologien um eine Verbindung zum Fahrzeug herzustellen.
E: Ja, also was so also generell, da bin ich glaube ich auch nicht, nicht der Technologie-Experte, aber aus meiner Erfahrung - auch so aus anderen Supply-Chain-Themen wo man sich auch sehr viel von RFID, zum Beispiel, versprochen hat - kann ich nur sagen, dass das irgendwie auch eher hinter den Erwartungen zurückgeblieben ist.
Allerdings ist natürlich jetzt ein flächendeckender Web-Zugang dann ja irgendwie so ein IoT oder IIoT. Da ist natürlich auch jetzt, wenn man an sowas denkt, jede Ampel müsste jetzt da irgendwie Web Zu-

gang haben, natürlich auch schon für die Implementierung wahrscheinlich schwierig. Aber das ist tatsächlich ein spannender Punkt. Ja, das machen wir uns in unserem Use Case relativ wenig Gedanken zu, weil wir eher immer eigentlich davon ausgehen, das läuft einfach alles über übers Internet.
H: Wenn High-Level Ebene unterwegs und dann versucht man das ein bisschen runter zu brechen. Wie das denn tatsächlich umgebaut eingebaut werden könnte und dann stößt man auf diese Probleme.
E: Ja, genau.
H: Ich will noch kurz den Use Case an sich erweitern. Wir hatten es ja grad schon mal davon. Wir haben jetzt natürlich den Fahrzeughalter an sich. Also ich würde jetzt meinen Parkausweis an mein mein Auto übertragen. Wir haben auch gedacht, jetzt habe ich vielleicht noch zusätzliche Passagiere. Bei mir im Fahrzeug. Ich hätte zum Beispiel noch ein Passagier, der hat ja erstmal genau die gleichen Möglichkeiten wie ich. Das er sagt, er lässt sich selber auch Credentials ausstellen, von welcher Institution auch immer - Krankenkasse oder Einwohnermeldeamt, etc.. Und auch hier haben wir uns Gedanken gemacht, er könnte ja auch seine Credentials zusätzlich übertragen.
Über eine ähnliche Technologie und auch wieder. Vielleicht sogar auch nur temporär, dass man sagt, das ist erstmal begrenzt auf einen gewissen Zeitraum oder auf die Nähe, des Passagiers zum Fahrzeug, zum Smart Verhicle. Aber solange zum Beispiel der Passagier mit eingestiegen ist, mit drin sitzt, solange hat er zum Beispiel auch die Möglichkeit, eine neue, eine neue Anwohner Zone einzufahren. Könntest du dir sowas vorstellen? Dann praktisch. Mehrere Credentials von unterschiedlichen aus unterschiedlichen Quellen dann in einem Fahrzeug gesammelt?
E: Ja, ist auf jeden Fall eine spannende Idee. Da sehe ich tatsächlich halt auch wieder die Probleme, wie generell schon vom Owner-Transfer auf Vehicle. Also irgendwie so ein Credential-Chain / Proof-Chain wäre dann der Gedanke wahrscheinlich. Dass man dann im Grunde das Auto als eine Pool Wallet bezeichnen könnte, die dann die verschiedenen Credentials eben auch von verschiedenen Insassen hat, finde ich spannend. Wie viele Use Cases das explizit gibt, bin ich mir nicht so sicher, bei denen es tatsächlich auch relevant ist irgendwie Credentials von allen Insassen zu haben, aber wird es vielleicht auch geben. Jetzt irgendwie an der Grenze oder so zum Beispiel. Also was da noch viel relevanter zusätzlich wird, sind eben genau diese Punkte, die du auch schon kurz angesprochen hattest wie revocation, Verlässlichkeit. Also wenn du aussteigst, wirst du irgendwie tatsächlich dann automatisch auf die Revocation List geschrieben. Insgesamt würde ich sagen, da ist dieser Data Privacy Aspekt noch deutlich rel-

evanter für die Credentials.
H: Ja ist ein guter Punkt, auf jeden Fall. Wie siehst du das - Ich weiß nicht, wie das zum Beispiel im Bereich Logistik oder Supply Chain gelöst wird: Angenommen, ich würde jetzt einen Proof abfragen - das wäre dann auch ein Zero-Knowlegde Proof - und im einfachsten Sinne der Datensparsamkeit, würde es mir eigentlich auch nur reichen wissen. Ist das Credential vorhanden oder nicht. Ich glaube darauf könnte man es reduzieren. Dass man sagt, ich stelle einen Proof request an das Fahrzeug und egal was jetzt der Ursprung des Credentials in der Präsentation ist die er mir zeigt - ob vom Hersteller oder vom Owner oder vom Passagier - Sobald ein Credential da ist bin ich damit zufrieden und er darf fahren. Meinst du das ist ausreichend oder meinst du da müssten noch irgendwie zusätzlichen Informationen notwendig sein. Für so einen klassischen Access Fall.
E: Also weiß nicht genau, ob du das meinst. Ich könnte mir vorstellen, dass das Use Cases gibt, wo man nicht nur binär yes/no braucht, sondern eher auch so ein Range Proof. Das ist ja tatsächlich so ein klassischer Use Case, den man bei SSI eigentlich öfter hat. Irgendwie so ein Range Proof, dass man eben nicht „nur liegt überhaupt vor", sondern tatsächlich auch noch irgendwie „liegt innerhalb/außerhalb gewisser Bereiche" hat für so ein Proof. Ansonsten also falls es jetzt eher so um den wirkliche Proof oder das Credential geht, braucht man dann natürlich. Wie alle Informationen, die jetzt auch für die Verification notwendig sind. Das heißt je nach Implementierung aber halt so, vereinfacht gesprochen, diesen Public private Key Austausch, das heißt irgendwie Issuer-Key, sowie natürlich auch noch irgendwie ein Identifier in Richtung des Trust Ankers. Wo finde ich den, etc. Das sind dann ja aber alles Semantiksachen. Ich denke mal dort wird man sich dann auch an einem Standard orientieren, die ja gerade in Entwicklung sind. Ob jetzt ein, W3C-Standard ist oder wie auch immer. Aber dort sind ja standardisierte Protokolle, die dann in so einem Proof in einer Präsentation auf jeden Fall erhalten wären.
H: Das ist ein guter Punkt. Siehst du das Thema Standardisierung auch sehr zentral? Ich hatte jetzt schon paar Interviews, dass alle gesagt haben, Standardisierung ist ein absolutes Muss.
E: Ja klar. Also das ist, glaube ich, was uns auch alle so ein bisschen umtreibt gerade. Wird ja gerne verglichen mit der Entwicklung des World Wide Webs, was vielleicht ein bisschen zu hochgegriffen ist. Aber ähnliche Entwicklung ist jetzt für diese Credentialformate. Wie sehen wie Ps aus, wie sehen die Cs wie siehts aus, wie sieht ein Trust Anchor aus, wie verweist man darauf, hat man ein DIDnet hat man ein DIDCom. Hat man überhaupt DIDs? Ähm, da sind wir ja alle irgendwie gerade dran und für die allermeisten Use Cases ist tatsäch-

lich die Standardisierung auch mit der Hauptvalue, der drin steckt. Und wenn dann wieder jeder anfängt und sein eigenes System aufsetzt, auch jetzt in so einem Smart City Kontext, dann müsste man zumindest eine Interoperabilität zwischen den Standards gewährleisten, aber im Idealfall hat man natürlich irgendwie einen Standard, den solche Ps, Cs etc. folgen.

H: Okay. Das ist eigentlich so die extended Version von unserem Framework. Es gibt gewisse Design Objektes, die wir versuchen mit dem mit dem Framework abzudecken. Ich habe es am Anfang ein bisschen erwähnt, dass ist zum einen das Thema Überwachung der Umgebung. Das wir versuchen das zu verhindern, dass eben nicht mehr alle Unbeteiligten, die irgendwie in der Umgebung sind mitgetrackt werden. Gleichzeitig soll auch kein dauerhaftes Senden oder dauerhafte Profilerstellung von dem einzelnen Fahrzeug existieren. Und was wir uns überlegt haben ist, dass diese Delegation am Ende auch dazu führt, die Identität vom Fahrer und auch vom Vehicle ein bisschen zu trennen. Weil es ja jetzt aktuell auch so ist, dass durch die Nummernschildregister, die es gibt, mehr oder weniger alles in einen geworfen wird und die Fahrzeugidentität, dann kurzzeitig auch die Fahreridentität ist. Und ganz am Ende daraus folgend wäre es ja vielleicht sogar möglich, sogar die Zahl des Individualverkehrs zu reduzieren, weil man sagt, wenn ich es schaffe, meine Berechtigung oder meine Identität, in jedes beliebige Fahrzeug mitzunehmen und zu übertragen, dann sinkt vielleicht auch der Bedarf an eigenen Fahrzeugen, sondern wie schon angesprochen, sind diese Mietmodelle oder auch ja diese kurzfristig besorgten Fahrzeuge hätten dann auf jeden Fall noch mehr Nutzungsmöglichkeiten. Ist es deiner Ansicht nach durch so eine Architektur wie eben gezeigt möglich, dass man diese Objektives erfüllen kann?

E: Also links angefangen: Dieses Traffic Monitoring ohne das die Sorroundings gemonitort werden, würde ich tatsächlich sagen, ist voll erfüllt. Je nachdem wie man denn die Übertragung macht, aber die könnte man auf jeden Fall konzeptionelle so einrichten, dass man vom surrounding gar nichts mitbekommt. Das heißt, sei es jetzt über irgendwie wireless - sprich Übertragung per RFID - oder ähnliches. Wobei man dann natürlich wieder sagen muss, wenn jetzt alle wenn im surrounding irgendwas mit RFID ist, würde man das wahrscheinlich schon auch scannen. Das heißt, dann wäre so ein bisschen was vom surrounding auch erfasst, aber so Monitoring des Surroundings im Sinne von, man hat eine Verkehrskamera, die dann irgendwie auf Fußgänger oder Ähnliches filmt. Das hätte man natürlich Umgangen oder hätte man nicht mehr. Vor allem vielleicht auch das Wort „permanent“ hätte man auf jeden Fall adressiert, weil ja so eine Sache, des

SSI Paradigmas auf jeden Fall ist, dass man auch, ja den Grundsätzen folgend, der Austausch vom Holder aus initiiert wird.
Das wäre in dem Moment zu sagen, Ok das Vehicle ist dort und sagt, „lass mich durch“ und erst dann beginnt der Austausch. In der Praxis wird das wahrscheinlich, vielleicht nicht so ausgestaltet, weil man zum Beispiel jetzt die RFID Überprüfung einfach laufen lässt, sobald das Vehicle in den Bereich fährt. Aber grundsätzlich könnte man dieses „permanent“ wahrscheinlich auf jeden Fall eingrenzen und sagen, es wird nur ein expliziter Datenaustausch ausgelöst durch den Holder.
Das war tatsächlich auch für das zweite. Das da nicht permanent die Daten ausgetauscht werden müssen, sondern eben nur für den Austausch eine Verbindung hergestellt wird. Ja, insbesondere Location wäre jetzt tatsächlich für die Credentials auch – also kommt jetzt wieder auf den Use Case an – aber ansonsten wäre die Location auch relativ irrelevant. Ja für jetzt den Austausch.
Genau diese Trennung von den Credentials vom Fahrer und dem und dem Fahrzeug finde ich tatsächlich sehr spannend. Wie gesagt, muss man halt technisch abgebildet bekommen. Das man dann damit eben auch solche Prozesse vereinfacht wie Carsharing oder Ähnliches. Ja, da würde ich auch sagen, das ist auf jeden Fall erfüllt das Objective. Ich bin mir tatsächlich dann aber immer noch nicht ganz sicher, ob die Wallet beim Auto wieder wäre oder ob man dann eigentlich auch gar keine Verknüpfung braucht, sondern dass man dann. Sagt in einem Fall der Identifizierung oder Authentifizierung führt man das einfach einmal mit dem Fahrer und einmal mit dem Vehicle durch. Also dass man dieses Pooling der Credentials in einem Wallet was das Auto wäre gar nicht braucht, sondern dass man dann in so einem Miet-Case einmal sich gegenüber dem Vermieter mit seinen Credentials identifiziert und dann hätte man das schon mal abgehandelt und dann wären so Sachen, die über das Auto laufen, nur noch bilateral mit dem Auto auszutauschen. Das wäre tatsächlich dann eben die Frage für die Use Cases.
H: Genau. Ja, das ist sehr speziell. Ne, aber das sind auf jeden Fall Punkte. Ja, so viele Sachen, die ich noch nicht gedachte habe an dem Punkt.
E: Das ist tatsächlich ein sehr spannender Case, wo man irgendwie überlegt, ob irgendwie dann auch so Human Credentials in einer, von einem autonomen Agenten geführten, Wallet liegen und wie man das dann halt auch verwaltet. Genau, aber grundsätzlich reduction für Individual owned Vehicles. Also das ist natürlich ein sehr nachgelagerter Effekt, aber es kann das auf jeden Fall unterstützen, weil das meiner Meinung nach diese ganzen Leih-/Miet-/Sharing-Prozesse vere-

infacht. Man hat irgendwie in der Wallet kann die relativ einfach dann verifizieren, übertragen und damit solche Prozesse vereinfachen, ja.
H: Ja dank dir, auf jeden Fall. Eine Frage hätte ich noch, ob dir vielleicht mehr auf einer ja Datenschutz-politischen Ebene noch einfallen würde, ob überhaupt Bedarf da ist, für solche Datensparsamen Architekturen oder Frameworks? Siehst du da Bedarf oder glaubst du, dass das von politischer Seite eher nicht gewollt ist? Weil man, es profitiert ja irgendwo von der von der Überwachung.
E: Also von politischer Seite weiß ich es natürlich nicht, weil ich kein Politiker bin, aber wie momentan ja der Diskurs gefahren wird, ist es schon so, dass die Politik da auch sehr aware ist und auch sehr darauf bedacht ist. Aber Bedarf jetzt so von politischer Seite kommt, wenn dann, eben dadurch, dass sie von Bürgern darauf hingewiesen werden und ich persönlich sehe es als tatsächlich als sehr relevant an. Das gerade wenn man eben auch die Bevölkerung überzeugen möchte von einer voll digitalisierten Gesellschaft. Wir haben es ja auch mit „Bargeld oder nicht Bargeld“, wo auch einfach sehr viele Vorurteile oder schlecht informierte Menschen, irgendwie halt einfach Angst haben vor etwas, was sie halt auch vielleicht auch einfach nicht verstehen. Weil es auch inzwischen sehr abstrakt ist und man kann nicht einfach irgendjemanden mal nen Zero-Knowledge Proof erklären.
Das Problem wird man jetzt in immer mehr Bereichen eben bekommen, dass die Sachen so komplex sind, dass man irgendwann irgendwie die Leute hat, die da auch einfach darauf vertrauen müssen. Da ist tatsächlich so dieser Stamp „von der Politik abgesegnet“, schon relevant, würde ich sagen. Und gerade diese Privacy ist extrem relevant, weil wir auch gelernt haben, irgendwie mit jetzt vermasselten Einführungen von e-Personalausweis und ähnlichem, dass wenn man einmal dieses Vertrauen verspielt, man es auch sehr schwer nur wieder zurück bekommt. Oder eigentlich überhaupt nicht. Und dementsprechend ist man schon gut beraten, das von Anfang an auch wirklich als Design Objective mit aufzunehmen. Und sollte tatsächlich schon auch eine große Rolle spielen. Wenn auch, und das ist tatsächlich schon wieder so eine deutsche Sache, vielleicht nicht alles bestimmen und vielleicht auch nicht den Fortschritt komplett hemmen, sondern irgendwie in einem angemessenen Rahmen, einfach mit ins Design von solchen Lösungen einfließen.
H: Finde ich sehr gut was du sagst.
E: Dann ja, Privacy Preserving Technologies. Auch irgendwie neue Wege gehen, wie jetzt auch Zero-Knowledge Proofs oder ähnliches. Dass man eben halt beides hinbekommt. Digitalisierung aber ohne komplette Transparenz.
H: Ja, cool. Das war eigentlich schon von meiner Seite aus. Vielen, vie-

len Dank, dass du dich. Ja, relativ kurzfristig bereit erklärt hast, mir da zu helfen. Hast du noch irgendwie fragen oder? Ja, Fragen zum Ablauf, oder? Von deiner Seite noch irgendwas.
E: Nee, gerne hat Spaß gemacht, war ein cooler Case. Bin natürlich interessiert, was dabei rauskommt.

TRANSCRIPT: EXPERT F (GERMAN)

H: Sehr schön. Vielleicht würdest du mir gerade nochmal kurz erklären, was du deinen Schwerpunkt ist, wie du vielleicht zum Thema dezentrales Identitätsmanagement gekommen bist. Und lange du darin schon arbeitest?
F: Ja, aber ich bin erstmal [REDACTED]. Bin auch jetzt in meiner Promotion [REDACTED] seit. Ja, fast 2 Jahre n bisschen weniger promotionsthema geht n bisschen auch um dezentrales Management, ist fast sogar mehr der Fokus inzwischen gestartet, hat das n bisschen eigentlich mit dezentralen dezentralen Technologien Overall respektive mit Blockchain eigentlich initial. Was hat sich aber alles so ein bisschen entwickelt. Also ich glaube die wurde auch bewusst sein, was da so alles passiert ist in dem letzten halben Jahr, ja auch was die das 2.0 Regulatorik angeht und auch alles was mitschwingt. Mit dem I. Paradigma. Und da war ganz zu Beginn relativ oft zumindestens bei Design irgendwo so. War es so geregelt, dass halt viel auch auf Blockchain Basis gemacht wurde? Zumindestens Register und Revocation et cetera und so weiter angeht? Ich glaube das hat jetzt noch ein bisschen. Geändert und so ist das auch nochmal ein bisschen sich in meinem Promotionsthema vorangeschritten, indem sie sich halt einfach die Themen zueinander verhalten. Und O. Ist einfach so, dass mein Promotions Thema hat, sich anschaut was Herausforderungen sind für dezentrale Technologien beziehungsweise Emerging Technologies und in die Praxis zu überführen zu werden und dementsprechend orientiert sich so ein bisschen auf die Inhalte, auf die ich meinen Fokus lege. So ein bisschen damit, wie es auch in der sich in der Praxis entwickelt und. Wie einfach die ja Umstände durch Regulatorik oder marktwirtschaftliche Herausforderungen einfach eben Bedingungen wie solche Systeme eben gebaut werden. Müssen, auch wenn es nicht unbedingt das ist, was man immer gerne hätte, als Entwickler. Genau, Regulatorik ist eben wichtig und daran orientiert sich natürlich dann auch am Ende die Architektur so n bisschen. Genau das ist eigentlich ein bisschen da. Ich komm, vielleicht studiere ich Medien, Informatik Master, hatte aber mein Fokus eigentlich ganz anders drauf. Das hat sich so ein bisschen eigentlich während der Promotion doch wegen einer wissenschaftlichen Hilfskraft Zeit so ein bisschen gewandelt. Aber genau in dem Themenfeld, dementsprechend schon ein bisschen länger unterwegs.
H: Cool auf jeden Fall einen interessanten Punkt, gerade wenn du sagst, hier das überführen in die Praxis, ich glaube das ist bei bei meinem Thema auch relevant. Ich würde kurz mal meinen Bildschirm teilen und ein paar Folien zeigen.

F: Ja, ich denke mal, gerade bei diesen SA dezentrales Management Thema ist glaube ich die Überführung in die Praxis so das was da so am prägnantesten irgendwo ist, ne? Ich glaub, wenn rechts und links schaut, ist es ja eben der Wunsch, quasi beispielsweise Digitalisierung von Personalausweisen et cetera auf Digital Wallet und so weiter bekommen und das ist ja stand heute zumindest in Deutschland und in vielen Mitgliedstaaten der EU noch nicht. So deswegen, das Thema wird glaube ich immer wieder begegnen, wenn man sich mit. Thema an sich beschäftigt.
H: Ja, also die Versuche, die unternommen wurden in den letzten Jahren, die waren ja nicht fruchtbar. Und das auch.
F: Noch. Ich glaube immer, dass so bei jedem ist, die Schaufenster, Projekte oder was es auch immer war, ich glaube immer mindestens mal eine Kernerkenntnis konnte man ziehen. Ich glaube das Wichtige ist einfach, dass man in der Hinsicht einfach nicht den Kopf in den Sand steckt, sondern hat immer das Positive mitnimmt und dann neu anläuft. Irgendwie 200 das Quatsch ist, von vornherein alles zu verteufeln. Ich glaube, da gibt es ja genug Konsorten, die da immer wieder drauf hauen. Aber keine Lösung ist auch keine Lösung, so finde ich. Komisch an dieser Diskussion.
H: Kritisieren ist immer einfach, das ist aber irgendwas zu entwickeln oder irgendwas Neues auf den Markt zu. Bringen, das ist halt die Kunst.
F: Ja da beziehungsweise man muss sich die Frage stellen, einfach mal 2022 das noch nicht digitalisiert hat.
H: Auf jeden Fall siehst du meine. Folie ja, ja, perfekt. Kurz noch ein bisschen was zum Hintergrund. Wir haben uns ein bisschen mit dem Thema Identität im Straßenverkehr und auch in Smart City bisschen beschäftigt. Wir hauptsächlich auch sehen, dass der Trend immer mehr zu zu Smart Cities geht, das heißt, dass immer mehr Technologie im Alltag, im Straßenverkehr. Du hast immer mehr, ja tatsächlich auch Überwachung im Sinne von Verkehrs Kameras installiert. Es wird auch teilweise die Fahrzeuge an sich senden, ihre ihre Position fast dauerhaft an Dritte. Das ist ein Trend, den wir zum einen sind, zum anderen sehen wir aber auch, dass es immer mehr anwendungs Gründe und Anwendungsfälle auch gibt für Städte, zum Beispiel Umweltzonen einzurichten oder eben auch in London ist das ein gutes Beispiel, so High Traffic Zones. Oder Anwohner Zonen. Wo auch ein gewisser Bedarf da ist, Fahrzeuge zu infizieren und auch ein gewisses Monitoring einzuführen. Und eben. Ja, diese Technologie noch anzuwenden. Das ist ein Trend, ja, den sehen wir fast weltweit steigend. Was wir uns überlegt haben, es gibt ja schon einige bedenkliche Punkte an in dem Fall. Also gerade was der Punkt Datenschutz

angeht bei Verkehrs Kameras die eine komplette Straße überwachen werden ja nicht nur die Fahrzeuge erfasst, die wirklich relevant sind für den für den eigentlichen News, sondern auch Fahrradfahrer, auch Fahrzeuge die vielleicht nur die Straße kreuzen. Und das ist zum Beispiel auch was, was uns da sehr, sehr bedenklich vorkommt. Deswegen haben wir uns überlegt, diese Form von Identifikation auch ein bisschen zu dezentralisieren und da auch n ja mit den aktuellen Technologien, die es so gibt. Diese einzuführen.
F: Meine Frage vorweg, so ein bisschen ja, das läuft ja nicht nur über Verkehrs kameras. Also das ist ja meistens auch so, dass also vor allem im Lieferverkehr, bei LKW, und das werden wahrscheinlich die Maschinen sein, die da irgendwie relevant werden, um irgendwie die Missionen. Nochmal deutlich mehr zu senken. Wahrscheinlich bei privat P wird es funktionieren, aber das ist ja oft so, dass man quasi auch eine gewisse Maschinennummer einfach auslesen kann und dafür nicht zwingend eine geraucht. Also könnt ihr beispielsweise irgendwie den oder teilweise läuft das so, dass wir auch beim das ist irgendwie das Bundesamt für Logistik und Mobilität in Deutschland, die fahren teilweise. Physisch neben den LKWS auf der Autobahn her und können den Chip dann von denen einscannen. Von Auto zu Auto werden die fahren, also theoretisch ist nicht immer, könntest wahrscheinlich selektiv einfach einstellen, dass nur ein spezieller Typ von Maschinen. Daten eingescannt oder getrackt werden soll zumindest nicht über machen.
H: Tatsächlich ist ein einer der wichtigen dieses Vehikel Vehikel Communication beziehungsweise Vehicle to können wir gleich noch drauf, auf jeden Fall gut. Da sehe ich halt auch tatsächlich die Notwendigkeit zu verhindern, dass dauerhaft diese diese Vehikel Nummer mit der aktuellen Position übertragen wird. Eben aus der Kritik heraus, da bewegungs. Profile zu erstellen. Ich habe gerade schon erwähnt, wir haben uns überlegt ein kleines Framework da draus zu bauen. Vom Grund Aufbau her. Es, wenn aus der SI Ecke kommt relativ selbsterklärend. Also wir haben sowas wie public institutions. Das können Meldeämter sein, jetzt, die zum Beispiel einem Anwohner ne melde Adresse attestieren. Das können aber auch Gutes, zum Beispiel Krankenkassen, die einem Bescheinigung für Beeinträchtigungen attestieren. Und im Prinzip ist das ein ganz normaler Issuer, wie man ihn kennt, der einem in welcher Form auch immer, ein Credential ausstellen kann. Was jetzt dazukommt, dass zum Beispiel das Gleiche auf einer Fahrzeug Ebene, das heißt, wir haben einen einen Herstellern, der einem Smart Vehicle oder einem modernen Vehicle im Allgemeinen gewisse ebenfalls ausstellen kann, das gleiche Spiel Aussteller für das für das Vehikel, das können eben genau solche Sachen sein

wie. Eindeutige, ja eindeutige Kennzahlen. Relevant für Umweltzonen sind wahrscheinlich in der Emissions Parameter oder oder Bauteil Parameter die im Fahrzeug ne gewisse. Ja, Umweltfreundlichkeit, alles Tieren, das wären zum Beispiel die so ein Fahrzeug relevant sind. Was jetzt neu dazukommt, ist eine Form von Integration. Das heißt, mein Fahrzeug erhält nicht nur seine seine eigenen Pentiums, sondern hält dazu auch noch die Möglichkeit, die Credentials vom Halter aufzunehmen. Das heißt, ich kann als Besitzer zu meinem Fahrzeug hingehen und sagen, ich fand sowieso jeden Tag damit. Ich übertrage ihm. Jetzt die meinen Parkausweis zum Beispiel. Und dann wird dieser Parkausweis oder der Nachweis für meinen, für meinen Wohnort wird dann im Fahrzeug gespeichert. Mit dem Hintergrund.
F: Weiß was man will, zwingend also meinen Wohnsitz auf meinem Park oder auf meinem Auto zu speichern, würde ich nicht machen oder nicht unbedingt wollen, während ich meinen Parkausweis selber schon. Mit dem Partner Fahrzeug verbinden würde. Also warum braucht man die Wohn Adresse dafür?
H: Muss nicht die Adresse sein. Parkhaus ist wahrscheinlich der Haupt Cast dafür. Das ist natürlich sehr n kleines Beispiel aus der Praxis habe ich zum Beispiel bei mir, so, dass die packungs Weise an gewisse Zonen in der Stadt gebunden sind, das heißt? Vielleicht, was ich aktuell mehr oder weniger in Papierform mühsam ausdrucken muss oder mein Passwort legen muss. Oder wenn ich ein anderes Fahrzeug benutzt, dann. Mitnehmen muss, könnte ich jetzt in digitaler Form mehr als geschlossen lassen. Und dann Fahrzeug delegieren, so dass mein Fahrzeug dann bei Bedarf, wenn ich hier mit der mit der Infrastruktur zum Beispiel kommuniziere, einfach personelle Puff abfragen darf. Darf ich hier überhaupt in diesem in diesem Bereich parken oder nicht?
F: Ja, also ich glaube schon. Also grundsätzlich finde ich das mega gut, die Idee dazu, aber ich glaub ich sogar noch ein paar, könnte auch zum Beispiel sowas denken wie. Wie heißt das, diese Plakette, die zeigt, ob man irgendwie die. Die Umwelt Plakette genau oder man könnte zum Beispiel auch, wenn man die Vignetten aus Österreich oder Schweiz denkt, also solche Sachen gibt es. Ja, schon. Wo man irgendwie das Auto theoretisch mit Credits ausstatten könnte, die ich aber nicht zwingend personenbezogen machen würde. Wahrscheinlich. Dann bedarf nicht so sehr zumindestens. **H**: Genau können wir gleich noch. Zu aber für sowas. Genau sowas ist eigentlich gedacht, also die Möglichkeit, dass das Auto mit einer Infrastruktur kommunizieren kann. Das kann alles möglich sein. Das kann eine Straßenlaterne seine Ampel sein, einfach bei Einfahrt, dass wir hier nähert sich einem Infrastruktur. Ja, gebildet oder Mechanik? Dort passiert

eben dieser, dieser Prüf request und auch diese diese Präsentation, idealerweise Datensparsamkeit, Synology Proof. Und da wird dann durch eine durch entscheidungs Logik abgebildet. OK, dieser dieser Einfall ist valide oder das Fahrzeug darf hier parken, weil es zum Beispiel in einer Zone für beeinträchtigte Menschen, dass dann mit seiner blauen Plakette durch das da auf dem Platz stehen.
F: Ja ok.
H: Das wäre dann so ein Fall. Da sind wir dann wieder bei K. Personenbezogenheit ja, nein.
F: Okay. **H**: Soweit aber verständlich?
F: Ja, also ja nur. Da frage ich mich halt nur so ein bisschen, wenn man das eh schon Personalchef löst. Ja, also das war vielleicht der einzige Zoo personenbezogene Fall, der jetzt anfangen würde mit behinderten Ausweis ja oder nein? Wobei ich mich auch frage, wenn man das jetzt offenlegen würde, ob. Das schlimm ist. Man schreibt ja nicht, was man für eine Behinderung hat oder in irgendeiner irgendeiner Form, sondern nur, dass man es da gut, aber erstmal weiter.
H: Nee, alles gut. Input ist immer sehr gut. Vielleicht auch die Frage, ob das so vom Grund Aufbau her verständlich ist oder ob es da irgendwo kritische Punkte siehst, die die irgendwie dagegensprechen gegen diesen grundlegenden Aufbau.
F: Ja, bisher noch nicht.
H: Was auch überlegt hatten, war eine kleine Erweiterung von diesem News Case. Wenn ich zum Beispiel als Fahrzeughalter nicht der einzige bin, der in dem Fahrzeug fährt, sondern das Ganze zum Beispiel noch über einen Passagier erweitere. Und jetzt zum Beispiel auch die Möglichkeit habe. Ich habe einmal die Möglichkeiten das des Fahrers und die Berechtigung in gewisse Areale einzufahren, aber auch gleichzeitig die Berechtigung, dass das Passagiers. Der dich ja genauso ausstellen kann und dann auch genauso über Delegation, Prozess, praktisch das gleiche Fahrzeug übertragen kann. Das heißt? Das Fahrzeug wird mehr und mehr zu einer Art Pool, der diese. Diese Credentials irgendwo verwaltet. Und eben bei Bedarf. Dass das entsprechende Schreiben kann.
F: Was war da zum Beispiel für?
H: Ein Beispiel dafür wäre zum Beispiel. Ich darf mit meinem Fahrzeug vielleicht nicht mich auf den behinderten Parkplatz stellen, aber ich habe mein Passagier dabei, der ist. Der Staff. Und er kann sein genauso an mein Fahrzeug übertragen. Wie ich selber tue. Was ist also der größere Use Case? Wäre dann auch dahingehend zu sagen, ich kann viel viel mehr oder viel flexibler die Berechtigung von. Fahrer und Mitfahrer an ein Fahrzeug übertragen und bin und bin ungebunden von dem eigentlichen Fahrzeug. Ich kann Fahrgemeinschaften bilden,

die dann die Berechtigung zusammenlegen können.
F: Ja, war es gut. Ja, aber wie läuft das heute aktuell? Das ist wahrscheinlich so, dass. Diejenige Person, wahrscheinlich eine Art Betreuerin, Betreuer. J, die wahrscheinlich diese Plakette irgendwie auf ihr Auto gebunden haben und dann sie selten k.
H: Genau das, das ist eine sehr starke Kopplung zwischen Ja der der Person mit der ausgestellten Daten und dem eigentlichen Fahrzeug. Und genau das sehen wir im Prinzip auch schon bei Nummernschild Überwachung zum Beispiel. Ich fahre durch eine Strafe, die Kamera scannt das Kennzeichen und bindet eigentlich das Kennzeichen an den Fahrzeughalter, weil der Fahrzeughalter in einer zentralisierten Registry steht, in einer zentralisierten Datenbank.
F: OK.
H: So schaffe ich es praktisch, das immer mehr zu ent koppeln und auch eine gewisse Datensparsamkeit auch zu erhalten. Auch das soweit verständlich. Ja, also.
F: Ja, alles gut.
H: Genau siehst du da auch irgendwo, gerade bei diesem Delegation. Party ist eigentlich das, wo die meisten sagen, das ist, das ist schwierig mit den aktuellen Technologien. Hast du dich damit schon mal beschäftigt mit dem Thema delegieren von Credentials?
F: Ja, habe ich tatsächlich auch in meiner Masterarbeit damals. Da ging es nämlich darum, dass wir nahtlos nahtloses Ticketing System bauen wollten. Und da haben wir uns auch gefragt. Also die Idee ist ja dann zu sagen, wenn ich jetzt irgendwie von Frankfurt nach London Reise, dann würde ich typischerweise von meiner Haustür irgendwie. Vielleicht mit dem Bus zum Bahnhof fahren, vom Bahnhof zum Flughafen und dann zum Flughafen, irgendwie nach London fliegen, also mal mindestens 3 oder voraussichtlich 3 Transportwege. Und wenn ich das jetzt buchen wollen würde, müsste ich wahrscheinlich bei jedem Anbieter einzeln buchen. Also ich könnte jetzt nicht irgendwie in App gehen und sagen, ich hätte gern diese reisestrecke und dann würde ich irgendwie ein Angebot kriegen, wo ich direkt ein Ticket bekommen. Was für alle. 3. Also klar, es gibt Pauschalreisen oder so. Für den erstmal Nahverkehr in Kombination mit Fernverkehr. Und da ist auch die Idee gewesen, wie kriegt man das denn theoretisch hin, dass man doch irgendwie weiß, nicht bei der Deutschen Bahn den Buchungsprozess, also die die Buchung für die Reise machen kann und beispielsweise Lufthansa delegiert dann entsprechend ein Ticket die Bahn, damit die das quasi. Ja, ausstellen können Turns out ist natürlich nicht cool aus einer Marktperspektive, weil die Lufthansa natürlich irgendwie den direkten Kundenkontakt haben möchte, worüber wir dann am Ende natürlich dann, oh Wunder, auch mit einem SI Lö-

sungen gelöst haben, die dann halt die bilateralen Kommunikationskanäle zwischen. Kunden und. Mobilitäts Dienstleister einfach herstellt und dann quasi durch eine gewisse Weiterleitung an den jeweiligen Mobilitäts Dienstleister das Ausstellen des jeweiligen Tickets dann auch in so einem Batch Format durchführen kann, entsprechend schon draußen aber noch keine sinnvolle Umsetzung dafür gefunden. Ich glaube auch als ich mich damals beschäftigt hatte, war auch diesen ganzen Delegation Funktionalitäten zumindestens die auch noch nicht. Auf dem Stand, dass man es hätte ordentlich benutzen können. Ich weiß nicht, wie das inzwischen.
H: Aber immer noch nicht.
F: OK, bei meiner Aris in die Version war glaube ich auch 0.0.03 oder irgendwie sowas, also wahrscheinlich inzwischen auch noch mal anders. Dementsprechend kann ich mir schon gut vorstellen, dass das geht. Im Zweifel funktioniert das aber wahrscheinlich auch über so ne. Jetzt gerade den Namen vergessen und ich glaube x 307 Weiterleitung wo man auch über QR Codes einfach auf die Wallet entsprechend weitergeleitet wird. Und also theoretisch. Wobei zwar nicht natürlich. Irgendwie müsst ihr wahrscheinlich das Auto. Die Credentials ausgestellt bekommen. Richtig also in diesem Delegation Vorgang müssten ja quasi die die Public situtionwürde den behinderten Ausweis im Zweifel ausstellen und der Vehicle oder Passenger müssten ja irgendwie dann dem Auto. Bin auf dem Ausweis ausstellen, das ist doch die Idee, oder?
H: Ja. Entweder ausstellen. Was wir uns überlegt haben, so eine Kaskadierung von von den von den Zertifikaten, haben praktisch von der Zertifikats Kette baut und man dann am Ende nachvollziehen kann. OK, das Gesetz wurde von dem auch einer weitergegeben und signiert und der hat es von der Public Institutionen wirklich ausgestellt bekommen. Und wo? Dass man diesen Delegation Prozess dann als Tifikate legt.
F: Der also ich denke jetzt gerade in der technischen Fragestellung einfach, also wie kriegst du am Ende das Zertifikat aufs Auto prozessual? Und wenn ich Zertifikats kriege höre, denke ich sofort an x 509 und das wäre jetzt nicht zwingend quasi. Also ich weiß nicht, was ihr euch das jetzt hier überlegt, ob es jetzt wirklich mit in die Ares ist und dementsprechend.com oder mit irgendwelchen anderen Kommunikationsprotokollen. Also irgendwie musst du ja im Zweifel das Credential auf das Smart Wear bekommen. Und das wir jetzt mal ein bisschen was machen wollte. Wenn ich jetzt beispielsweise in diesem. Share Driving oder wie nennt man das Carsharing? So auch aus diesem. Aus dieser Welt jetzt komme und jetzt überlege, wie könnte man da quasi Daten abrufen, dann würde man vielleicht

einen statischen QR Code irgendwie aufs Auto kleben. Denn scannen kann, damit man im Zweifel irgendwie. Dann Profi Cash bekommen, Führerschein oder Perso oder so. Wenn man das übertragen hat, geht das Auto auf oder whatever. Solche Sachen aber so wäre es jetzt quasi andersrum. Oder man würde jetzt versuchen, quasi wenn der Vico, ohne dass einmal ausgestellt bekommen hat, von der Public Institution von Digital Wallet des Nutzers, das jetzt aufs Auto noch mal nachträglich zu bekommen. Also es war ja quasi SU go sein, also nächstes Person den behinderten Ausweis hat sich. Spontan entscheidet, mit dem Auto mitzufahren und dann quasi das Quentia übergeben möchte. Dann muss das ja nahezu in Echtzeit sofort irgendwie im Auto passieren können.

H: Also gerade dieser von. Mensch zu Fahrzeug, sag ich jetzt mal. Das ist tatsächlich noch ein Programm, so ein Prozess, der Ausschuss angestoßen werden muss und wahrscheinlich über eine Smartphone App mit in Verbindung zum zum Fahrzeug. Wer sagt, vielleicht sogar auf Request hier da? Ist ein Mensch, der hat Real für. Mich einmal ein Handshake zum zum identifizieren. Und dann eben die Möglichkeit. Zu werden verlegt werden soll.

F: Ja, also ich meine Zweifel. Es ist halt wie du schon sagst, musst du dann halt irgendwie dein Handy oder so am Auto anschließen können und mit dem Handy dann den QR Code scannen. Oder zumindest übergeben können per Link. Im Zweifel wird es schwierig, wenn du von deinem Handy QR Code scannen willst. Das ist schwer, weil geht nicht. Aber grundsätzlich finde ich die Idee auf jeden Fall mega cool und hilft da glaub ich auch noch ein bisschen Spontanität und das ganze Reinzubekommen.

H: Hast du dich mal mit einem Thema Smart City oder so auseinandergesetzt? Zufälligerweise.

F: Ja, ich hatte oder wir hatten mal ein Projekt dazu, wo es quasi darum ging, so Gated Areas mit dem SA quasi auszustatten. Also so im Sinne von. Gewissen Gebäuden, also den Bewohnern gewisser Gebäude in diesen gated areas, halt die entsprechenden Kredite zu geben, einfach das Gebäude zu betreten. Für parking Zonen und so weiter und auch überhaupt Negara reinzukommen hat sie dafür so ein bisschen, aber jetzt nicht im Gesamtkontext Smart City so aber. Das ist wahrscheinlich einfach nur kleinere Version davon ein bisschen.

H: Ja, also auch da hat man überlegt, was da die besten Übertragungswege. Wir haben uns gesagt, der klassische Fall ist eine Art induktionsschleife oder irgendwo ne Bluetooth Verbindung oder vielleicht sogar ein kleines kleines Wlan Netz aufzubauen. Und dann eben auch diese Kommunikation mit der mit der Infrastruktur zu ermöglichen,

dass das relativ schnell dann drahtlos aufgebaut werden kann und auch dann die Kanäle dann für die übertragen werden.
F: Also ich glaube, dass tatsächlich relativ viel auch schon gut über statische QR Codes zu geht oder J Codes oder was ist da alles für? Unterschiede gibt. Wo du sogar nicht zwingend. Also klar, du brauchst natürlich irgendeine Verbindung. Wahrscheinlich Bluetooth, NFC oder irgendwie sowas halt anbietet, aber da geht schon relativ viel glaube ich offline. Weil ich glaube, mit dem mit der WLAN Idee wird man schneller an seine Grenzen geraten.
H: Ja, also mit Sicherheit.

BIBLIOGRAPHY

[1] ADEME. *Anzahl der Umweltzonen in Europa in den Jahren 2011 bis 2020*. Sept. 2020.

[2] Mahmood A Al-shareeda, Mohammed Anbar, Iznan H Hasbullah, Selvakumar Manickam, Nibras Abdullah, and Mustafa Maad Hamdi. "Review of Prevention schemes for Replay Attack in Vehicular Ad hoc Networks (VANETs)." In: *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*. 2020, pp. 394–398. DOI: 10.1109/ICICSP50920.2020.9232047.

[3] Mamdouh Alenezi and Mohammad Zarour. "On the Relationship between Software Complexity and Security." In: *International Journal of Software Engineering & Applications* 11.1 (Jan. 2020), pp. 51–60. ISSN: 09762221. DOI: 10.5121/ijsea.2020.11104.

[4] Muhammad Asim, Jorge Guajardo, Sandeep S Kumar, and Pim Tuyls. "Physical unclonable functions and their applications to vehicle system security." In: *VTC Spring 2009-IEEE 69th Vehicular Technology Conference*. 2009, pp. 1–5.

[5] Clara Benevolo, Renata Paola Dameri, and Beatrice D'Auria. "Smart Mobility in Smart City." In: *Lecture Notes in Information Systems and Organisation*. Vol. 11. Springer Heidelberg, Jan. 2016, pp. 13–28. DOI: 10.1007/978-3-319-23784-8{_}2. URL: http://link.springer.com/10.1007/978-3-319-23784-8_2.

[6] Alethea Blackler, Vesna Popovic, and Doug Mahar. "Intuitive Interaction Applied to Interface Design." In: (Aug. 2005).

[7] Muhammad Burhan, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey." In: *Sensors* 18.9 (2018). ISSN: 1424-8220. DOI: 10.3390/s18092796. URL: https://www.mdpi.com/1424-8220/18/9/2796.

[8] H Varun Chand and J Karthikeyan. "Survey on the role of IoT in intelligent transportation system." In: *Indonesian Journal of Electrical Engineering and Computer Science* 11.3 (2018), pp. 936–941.

[9] Pedro Henrique Dias Valle, Lina Garcés, and Elisa Yumi Nakagawa. "A typology of architectural strategies for interoperability." In: *ACM International Conference Proceeding Series*. Association for Computing Machinery, Sept. 2019, pp. 3–12. ISBN: 9781450376372. DOI: 10.1145/3357141.3357144.

[10] Mircea Eremia, Lucian Toma, and Mihai Sanduleac. "The Smart City Concept in the 21st Century." In: *Procedia Engineering* 181 (2017), pp. 12–19. ISSN: 18777058. DOI: 10.1016/j.proeng.2017.02.357. URL: https://linkinghub.elsevier.com/retrieve/pii/S1877705817309402.

[11] European Union. *EU Trusted Lists*. URL: https://archive.ph/VIwEx.

[12] European Union. *eIDAS Regulation*. URL: https://archive.ph/ntma2.

[13] Federal Office for Information Security. *BSI minimum standards (Section 8 (1) Sent. 1 of the German Federal Office for Information Security Act (BSI Act))*. URL: https://archive.ph/Y5HOM.

[14] Radhika Garg and Swati Gupta. "A review on internet of thing for home automation." In: *International Journal of Engineering Research & Technology (IJERT)* 8.10 (2020), pp. 80–83.

[15] Glasgow City Council. *Glasgow's Low Emission Zone now in force*. URL: https://archive.ph/U2SKb.

[16] Seda Gürses, Carmela Troncoso, and Claudia Diaz. *Engineering Privacy by Design*. Tech. rep.

[17] Sahriar Habib, Zawata Afnan, Sakib Chowdhury, Abu Mohsin, and Sarah Chowdhury. "Design and Development of IoT Based Comprehensive System for Emergency Assistance." PhD thesis. Aug. 2020.

[18] Alan Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. "Design Science in Information Systems Research." In: *Management Information Systems Quarterly* 28 (Mar. 2004), pp. 75–.

[19] Neeraj Kumar Jain, R. K. Saini, and Preeti Mittal. "A Review on Traffic Monitoring System Techniques." In: *Advances in Intelligent Systems and Computing*. Vol. 742. Springer Verlag, 2019, pp. 569–577. DOI: 10.1007/978-981-13-0589-4{_}53. URL: http://link.springer.com/10.1007/978-981-13-0589-4_53.

[20] Danish Javeed, Umar Mohammedbadamasi, Cosmas Obiora Ndubuisi, Faiza Soomro, and Muhammad Asif. *Man in the Middle Attacks: Analysis, Motivation and Prevention*. Tech. rep. 7. 2020, pp. 52–58. URL: www.ijcncs.org.

[21] Anushree Joshi, Pradnya Gaonkar, and Jyotsna Bapat. "A reliable and secure approach for efficient Car-to-Car communication in intelligent transportation systems." In: *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, Mar. 2017, pp. 1617–1620. ISBN: 978-1-5090-4442-9. DOI: 10.1109/WiSPNET.2017.8300034. URL: http://ieeexplore.ieee.org/document/8300034/.

[22] Mostafa Haghi Kashani, Mona Madanipour, Mohammad Nikravan, Parvaneh Asghari, and Ebrahim Mahdipour. "A systematic review of IoT in healthcare: Applications, techniques, and trends." In: *Journal of Network and Computer Applications* 192 (2021), p. 103164.

[23] Mohamed Rawidean Mohd Kassim. "Iot applications in smart agriculture: Issues and challenges." In: *2020 IEEE conference on open systems (ICOS)*. 2020, pp. 19–24.

[24] Sarbjit Kaur and Sukhvir Kaur. *An Efficient Approach for Number Plate Extraction from Vehicles Image under Image Processing*. Tech. rep. URL: www.ijcsit.com.

[25] Richard Kirk. "Cars of the future: the Internet of Things in the automotive industry." In: *Network Security* 2015.9 (2015), pp. 16–18. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(15)30081-7. URL: https://www.sciencedirect.com/science/article/pii/S1353485815300817.

[26] Knud Lasse Lueth, Fernando Brügge, Mohammad Hasan, and Matthieu Kuleza. *State of IoT – Spring 2023*. Tech. rep. 2023.

[27] Suk Kyu Lee, Mungyu Bae, and Hwangnam Kim. "Future of IoT Networks: A Survey." In: *Applied Sciences* 7.10 (2017). ISSN: 2076-3417. DOI: 10.3390/app7101072. URL: https://www.mdpi.com/2076-3417/7/10/1072.

[28] Kim Mens, Rafael Capilla, Herman Hartmann, and Thomas Kropf. "Modeling and Managing Context-Aware Systems' Variability." In: *IEEE Software* 34 (July 2017), pp. 58–88. DOI: 10.1109/MS.2017.4121225.

[29] Volodymyr Miz and Vladimir Hahanov. "Smart traffic light in terms of the cognitive road traffic management system (CTMS) based on the Internet of Things." In: *Proceedings of IEEE East-West Design & Test Symposium (EWDTS 2014)*. 2014, pp. 1–5. DOI: 10.1109/EWDTS.2014.7027102.

[30] Edward E Ogheneovo and others. "On the relationship between software complexity and maintenance costs." In: *Journal of Computer and Communications* 2.14 (2014), p. 1.

[31] Jose Orlando and Montes De La Barrera. *A Historical View of Smart Cities: Definitions, Features and Tipping Points Working Paper*. Tech. rep. 2020. URL: https://ssrn.com/abstract=3637617.

[32] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. "A design science research methodology for information systems research." In: *Journal of Management Information Systems* 24.3 (Dec. 2007), pp. 45–77. ISSN: 07421222. DOI: 10.2753/MIS0742-1222240302.

[33] Alex Preukschat, Drummond Reed, Christopher Allen, and Fabian Vogelsteller. *Self-Sovereign Identity*. Manning Publications Co., 2021. ISBN: 9781617296598.

[34] PwC. *Prognostizierter Anteil von vernetzten Automobilen (connected cars) in den USA, China und der EU von 2020 bis 2035*. 2020.

[35] Carmen ROTUNA, Alexandru GHEORGHITA, Alin ZAMFIROIU, and Dragos-Marian SMADA. "Smart City Ecosystem Using Blockchain Technology." In: *Informatica Economica* 23.4/2019 (Dec. 2019), pp. 41–50. ISSN: 14531305. DOI: 10.12948/issn14531305/23.4.2019.04. URL: http://revistaie.ase.ro/content/92/04%20-%20rotuna,%20gheorghita,%20zamfiroiu.pdf.

[36] Hamed Rahmani et al. "Next-generation IoT devices: Sustainable eco-friendly manufacturing, energy harvesting, and wireless connectivity." In: *IEEE Journal of Microwaves* 3.1 (2023), pp. 237–255.

[37] Rajiv. *What are the major components of Internet of Things*. URL: https://archive.ph/BKjmT.

[38] Carol Rivas. "Coding and analysing qualitative data." In: *Researching society and culture* 3.2012 (2012), pp. 367–392.

[39] Roland Berger. *Anzahl der von Städten veröffentlichten Smart City-Strategien weltweit in den Jahren von 2008 bis 2015*. 2017.

[40] Efat Samir, Hongyi Wu, Mohamed Azab, Chunsheng Xin, and Qiao Zhang. "DT-SSIM: A Decentralized Trustworthy Self-Sovereign Identity Management Framework." In: *IEEE Internet of Things Journal* 9.11 (June 2022), pp. 7972–7988. ISSN: 2327-4662. DOI: 10.1109/JIOT.2021.3112537. URL: https://ieeexplore.ieee.org/document/9536956/.

[41] Spyridon Samonas and David Coss. "The CIA strikes back: Redefining confidentiality, integrity and availability in security." In: *Journal of Information System Security* 10.3 (2014).

[42] Sebastian Sartor, Johannes Sedlmeir, Alexander Rieger, Tamara Roth, Sebastian ; Sartor, Johannes ; Sedlmeir, Alexander ; Rieger, and Roth Tamara. *Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets*. Tech. rep., pp. 6–18. URL: https://aisel.aisnet.org/ecis2022_rp/46.

[43] R M Savithramma, B P Ashwini, and R Sumathi. "Smart Mobility Implementation in Smart Cities: A Comprehensive Review on State-of-art Technologies." In: *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, Jan. 2022, pp. 10–17. ISBN: 978-1-6654-0118-0. DOI: 10.1109/ICSSIT53264.2022.9716288. URL: https://ieeexplore.ieee.org/document/9716288/.

[44] Martin Schanzenbach. *Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management*. Tech. rep. Munich: Technical University of Munich, Germany, 2020.

[45] Sovrin Foundation SSI in IoT TaskForce. *Self-Sovereign Identity and IoT*. Tech. rep. Aug. 2020.

[46] Manu Sporny, Dave Longley, and David Chadwick. *Verifiable Credentials Data Model v1.1*. 2022. URL: https://www.w3.org/TR/vc-data-model/.

[47] Manu Sporny, Dave Longley, and Markus Sabadello. *Decentralized Identifiers (DIDs) v1.0*. URL: https://www.w3.org/TR/did-core/.

[48] UN DESA. "Anteil der Bevölkerung in Städten weltweit von 1985 bis 2015 und Prognose bis 2050." In: (May 2018). URL: https://de.statista.com/statistik/daten/studie/37084/umfrage/anteil-der-bevoelkerung-in-staedten-weltweit-seit-1985/.

[49] Tim Weingärtner. "Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices." In: *The Journal of The British Blockchain Association* 4.1 (Apr. 2021), pp. 1–7. ISSN: 25163949. DOI: 10.31585/jbba-4-1-(5)2021. URL: https://jbba.scholasticahq.com/article/21244-identity-of-things-applying-concepts-from-self-sovereign-identity-to-iot-devices.

[50] Mark Weiser. "The computer for the 21st century." In: *ACM SIGMOBILE mobile computing and communications review* 3.3 (1999), pp. 3–11.

[51] Hakan Yildiz, Axel Küpper, Sebastian Göndör, Dirk Thatmann, and Patrick Herbke. "A Tutorial on the Interoperability of Self-sovereign Identities." In: (). DOI: 10.36227/techrxiv.20430825.v1. URL: https://www.researchgate.net/publication/362569152.

[52] Baozhu Zhou, Yuheng Liu, Yu Xie, Junpeng Wang, Zeqi Hao, and Jian Meng. "Research and Application of Intelligent Street Lamp Platform Based on Ubiquitous Internet of Things." In: *Journal of Physics: Conference Series*. Vol. 1920. 1. IOP Publishing Ltd, May 2021. DOI: 10.1088/1742-6596/1920/1/012068.