POPCORN

Privacy-Preserving Charging for eMobility

Master Thesis

10 January 2013

Christina Höfer
MSc Computer Science
Specialization Computer Security

Graduation committee:
Prof. Dr. F.E. Kargl (University of Twente & Ulm University)
Dr. J.Y. Petit (University of Twente)
Dr. E. Zambon (University of Twente)
Dr. R.K. Schmidt (Denso Automotive Deutschland GmbH)

UNIVERSITY OF TWENTE.

Distributed and Embedded Security
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente, The Netherlands

Abstract

As the demand for sustainable, low-carbon driving solutions is increasing, the electrification of vehicles, called electro mobility or short eMobility, is the next big milestone for the automotive industry. Vehicle manufactures, power grid operators and energy companies are devising approaches to integrate electrical vehicles with the power grid. Connecting electrical vehicles to the energy grid and the Internet poses several advantages for the driver, vehicle manufacturers and grid operators. Yet, these approaches need to be compatible, secure and privacy-preserving. This master thesis investigates the security and privacy challenges of electric mobility and focuses on the design, implementation, and evaluation of a privacy-enhancing charging solution for electric vehicles.

Contents

List of Abbreviations

CA	Certificate authority
CH	Clearing house
CRL	Certificate revocation list
CS	Charging station or charging spot
DR	Dispute resolver
EP	Energy provider
EV	Electric vehicle
EVCC	Electric vehicle communication controller
EVSE	Electric vehicle supply equipment; charging station
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MO	Mobility operator
OCSP	Online certificate status protocol
OEM	Original equipment manufacturer; vehicle manufacturer
PH	Payment intermediary or payment handler
PIA	Privacy impact assessment
PII	Personally identifiable information
PIT	Privacy-invasion type
POPCORN	Privacy-Preserving ChaRgiNg
SDR	Service detail record
SECC	Supply equipment communication controller
SPOF	Single point of failure
TLS	Transport layer security
TTP	Trusted third party
URI	Uniform resource identifier
V2G	Vehicle-to-grid

CHAPTER 1
Introduction

People and businesses want to stay mobile in the years to come despite fossil resources becoming more expensive. Hence, automotive manufacturers are investigating alternative propulsion systems. One alternative is a drive train which utilizes the electric engine. Electric engines have a higher energy efficiency than combustion engines and they do not produce exhaust emissions. In highly congested areas, such as cities, electric vehicles (EVs) can have a significant positive effect on the environment, especially if the batteries are charged by renewable electricity sources [6]. Vehicles which rely on electricity for their primary energy supply fall under the concept of electro-mobility, shortened to eMobility. This is also includes vehicles which utilize a range extender to actively recharge the battery [49].

A common criticism of electric vehicles is that they have short ranges and take a long time to charge [52]. For example, a domestic power supply currently takes a few hours to charge an empty EV battery. Therefore, it is suggested to charge EVs whenever they are parked so that the battery charge is maximized. Frequent charging requires that the charging and billing process is simple. A wide coverage of charging stations is needed to make recharging possible in various locations. Charging spots can be placed in private homes, on parking lots and integrated with existing gas stations. The electricity for charging the batteries can be provided by the existing power grid [14].

Other than the environmental benefits, governments and companies are analyzing the opportunities for new use cases to make electric driving more attractive [52]. They try to make electric vehicles a new and improved driving experience, for example, by using futuristic designs, features and materials. The key goals are usability, convenience and value-added services for the driver and passengers.

Another argument for the acceptance of EVs are the improvements to the power grid in the recent years. Communication between energy producers and energy consumers has been introduced to obtain almost real-time information about the energy demand and supply. This allows suppliers to better manage the power distribution and minimize losses. Electric vehicles are supposed to integrate with the power infrastructure to exchange electricity and data. Particularly the data exchange possibility offers new functionalities. Via the charging station the power grid can communicate with the vehicle to predict the energy demand. Future ideas include using the electric vehicles' batteries as temporary energy storage to overcome spikes in the energy supply and demand, and to instruct vehicles to charge overnight when the energy demand is low [26]. In order to implement these features, V2G communication is vital. For increased comfort, the payment process can be automated, so that the vehicle's energy costs are added to the driver's domestic energy bill. Vehicle manufacturers can make use of the interconnection while the vehicle is charging to perform remote-diagnostics or firmware updates. Also, third party value-added services can be offered during this time.

Communication between the electric vehicle and the power grid is referred to as vehicle-to-grid (V2G) communication. V2G communication is required to identify and authenticate a vehicle, coordinate the charging and discharging process, handle the billing, and to support the extra services. Therefore, communication needs to be an integral part of a charging infrastructure for electrical vehicles.

Various automotive companies are building prototype electric vehicles, while automotive suppliers

and electricity companies develop charging systems and run pilots to test their charging infrastructure [11, 12, 37, 92, 106]. In most cases however, each party has developed its charging systems independently. In order to have one coherent eMobility system, standards are being developed for the communication between the electric vehicle and the charging station, and for the communication between the charging station's smart meter and the power grid. However, the eMobility infrastructure details are not clearly defined. At the time of writing, there are no end-to-end electric vehicle charging protocols that handle the complete charging process and automated billing. The infrastructure has to allow secure and reliable transport of the electricity and data, while the communication protocols have to take security aspects into account, so that cheating of any involved party and tampering with (communication) data is impossible. The proposed designs for the charging infrastructure and communication protocols are taking the security requirements seriously. However, in addition to security measures, the privacy of the vehicle driver should be taken into account. As for smart metering [32, 68], electric tolling systems [96] or electronic payments [28, 66], privacy concerns arise for electric vehicle charging systems. While charging the vehicle is communicating with the infrastructure and privacy-sensitive data may be transmitted, such as vehicle identification, location data or billing details. Due to the frequent charging times, communication protocols have to be privacy-preserving to prevent tracking of individual vehicles or drivers by any of the involved parties. How the proposed protocols impact privacy is currently unknown. Most protocol versions ignore privacy or equated with confidentiality.

This thesis analyzes the possible eMobility infrastructure scenarios and investigates the privacy impact of vehicle charging and billing communication. Next, it proposes a privacy-preserving charging protocol based on the existing standardization efforts. Finally, the protocol is evaluated using a prototype implementation and comparison with existing approaches.

This thesis addresses the following research questions:

1. How does the eMobility infrastructure look like?
2. How privacy-preserving are existing approaches for electric vehicle charging and billing?
3. How can electric vehicles be charged and billed while preserving privacy?
4. How does the privacy-preserving protocol evaluate and compare with existing approaches?

This thesis is organized as follows: Chapter 2 gives an overview of eMobility, the infrastructure, the involved stakeholders, and the existing protocols. Further, the privacy concerns of the eMobility system are introduced and the focus of the thesis is defined. In order to develop a privacy-preserving charging protocol, the eMobility infrastructure needs to be defined. Chapter 3 discusses the requirements of the eMobility system and the relevant protocols. The privacy impact of electric vehicle charging and automated billing is investigated in Chapter 4. For this, a Privacy Impact Assessment (PIA) of the defined eMobility infrastructure with focus on the ISO/IEC 15118 electric vehicle charging protocol is performed. Next, Chapter 5 proposes POPCORN, our privacy-preserving charging protocol. The technologies used and the required changes to existing ISO/IEC 15118 protocol are discussed. The privacy properties and the feasibility of the POPCORN protocol is evaluated in Chapter 6. A PIA is conducted for the theoretical evaluation and a proof-of-concept is developed for the practical evaluation. The chapter ends with an overall discussion of privacy protection and the efforts it takes to realize it. Finally, Chapter 7 concludes this thesis.

CHAPTER 2

Problem Statement & Motivation

This chapter provides an introduction to the eMobility developments and discusses the state-of-the-art of eMobility in Europe and the envisioned future. The infrastructure and all relevant stakeholders are explained. Further, an introduction to the privacy concerns in eMobility is given. Finally, the focus of this thesis is discussed.

2.1 eMobility overview

The electro-mobility is a broader concept than electric vehicles alone. It makes use of the advances in the power grid infrastructure and utilizes the Internet and cellular network for the transport of messages and third party services. Communication between the vehicle, the charging station and the grid is an essential part. This section gives an overview of the beginnings of eMobility, the state-of-the-art and the goals that companies envision.

2.1.1 The beginnings of electric vehicles

The first electric vehicles were invented in the beginning of the 1800s, still before the rise of gasoline powered vehicles [7, 75]. Electric vehicles had many advantages over the widely used steam-powered and the still primitive gasoline-powered vehicles [94]. They were clean, silent, and simple to operate. In 1900 almost a third of all vehicles in the United States were electric. However, electric vehicles also had fundamental shortcomings compared to vehicles using other propulsion mechanisms. Electric vehicles were much slower and were severely limited by their battery range of 40 to 65 kilometers in the early years [94]. The batteries had to be recharged frequently and this took a long time. Further issues were caused by the nonexistent widespread charging infrastructure. Driving was only possible in local areas where recharge facilities were available. As combustion engine vehicles entered mass production and no technological improvements could be made to electric engines and batteries, the use of electric vehicles declined in the 1920s.

2.1.2 The move to smart grids

The earliest electrical grids were developed at the end of the 19th century. Multiple small local grids generated and supplied electricity to urban regions. In the 1920s, the isolated utility grids were interconnected to make use of economics of scale and to improve reliability [10]. Over the past century, the power grid kept growing as more power stations were connected, forming a large centralized, unidirectional power generation and distribution grid [10]. The power grid is demand-driven, i.e., the energy production is increased or decreased by turning on or off power plants as the demand increases or decreases. This process requires accurate knowledge about the current and near-future energy demand which is often estimated using electricity demand patterns [25, 47]. The

estimation of the energy demand and the management of the grid have become difficult tasks as the grid grows larger.

In the recent years utility companies have been demanding a modernization of the electricity grid. Since the beginning of the 21st century the grid is being transformed into a decentralized, digitally controlled, fully networked transmission system [41]. The improved grid will reduce losses in the power generation, makes distribution more effective, is more fault-tolerant, and allow real-time demand response [25,41,47,80]. The modernization is achieved by allowing a bi-directional flow of information and electricity between energy producers, distributer and consumers [24]. To do so, smaller sections of the power grid, often referred to as micro grids, are monitored by intelligent components that measure the energy production and consumption. This is referred to as the Advanced Metering Infrastructure (AMI). Also, more and more domestic homes and companies have smart meters installed. Smart meters are intelligent components of the AMI. The meters give electricity consumption readings to the energy distributors in intervals of one hour, so that the energy production can be coordinated more effectively. The modernized power grid is referred to as smart grid [65]. A general overview of smart grids is given in [39]. The security of smart grids has been studied by Falk and Fries in [47].

2.1.3 Current eMobility developments

Only in the 1990s when environmental efforts called for CO2-emission free vehicles the development of electric vehicles was revived [7]. However, the amount of electric vehicles in use in the European Union remains low. Currently, less than 1% of all vehicles are electric [37] and buying an electric car is more expensive than buying a combustion engine vehicle [52]. Nevertheless, many European states are investigating the eMobility opportunities and plan to invest in the development of an eMobility infrastructure [6]. A brief overview of these efforts is given next.

The Rijksuniversiteit Groningen has conducted a study [6] on electric driving in the Netherlands and offers recommendations for the Dutch national and local authorities to stimulate electric driving in the Netherlands. The limited availability and high purchasing costs of electric vehicles, as well as the unfamiliarity of motorists with the technology have been identified as one of the biggest barriers of advancing eMobility in the Netherlands. Further, it is assumed that the driving range of fully electric vehicles will never match that of internal combustion engine vehicles. Yet, in a small country like the Netherlands about 20 % of current motorists are potential candidates for electric driving since they have no need to high driving ranges. Further, the study emphasizes that Dutch authorities have limited power to influence eMobility, since it should be a European effort, so that no boarders are created by incompatible systems. Finally, the study examined a few pilot projects in various countries. Denmark and Israel have started a large scale introduction of electric driving. Denmark stimulates the sales of EVs by offering a 0% purchasing tax on zero-emission vehicles. In Israel the eMobility infrastructure is offered by the company Better Place. To decrease the purchasing cost and risks the company offers a subscription system for renting the electric battery, so that vehicle owners do not have to buy the battery.

The German government founded the Nationale Plattform Elektromobilität (National Electric Mobility Platform) [16] in 2010 to focus all eMobility efforts towards one electric driving system. The aim is to have one million electric vehicles on the road by 2020. The Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) has conducted and analysis of the eMobility challenges for the industry and the public authorities in cooperation with PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft [52]. The study examines the expectations and implication of eMobility on energy and vehicle suppliers, and end users. The analysis shows that a car is the most important means of transport and currently 81% of potential candidates would not buy an electric vehicle. However, 30% of urban motorist may consider electric vehicles in the future. For the energy industry the required investment in eMobility is higher than the earnings from selling electricity to EVs. Automobile manufactures see electrical vehicles still in the minority in 2020 with internal combustion engine cars remaining the majority.

In Germany, a pilot project has been started in 2008 by one of the largest energy suppliers RWE and vehicle manufacturer Daimler. At the point of writing about 500 charging spots have been

installed in Germany and another 200 spread over neighboring countries, such as the Netherlands, Luxembourg, Switzerland, Austria and Poland [82]. The RWE Mobility project aims to replace the charging plugs once the IEC/ISO charging standard has been finalized [37].

The impact of charging vehicles on the (German) power grid has been studied in [14]. A large amount of vehicles charging at the same time may cause grid overloading. However, if it is possible to recharge smaller amounts of electricity at multiple times during the day in various locations spread over a larger area, the current infrastructure is suitable without any alterations [14]. Also, using communication the vehicles can be instructed when to charge, so that only few vehicles charge during electricity demand peaks [26].

Beside economic stimulates to buy electric vehicles, also the common perspective that electric vehicles are less powerful than combustion engine vehicles and have short ranges needs to be changed [49]. The limited range concerns can be solved by providing a wide coverage of electric charging sports [14]. But until a functional and compatible infrastructure exists the sales of electric vehicles are likely to remain low [43]. On the other hand, it has also been suggested that the charging infrastructure developments are processing slowly because of the low amount of electric vehicles. This vicious circle remains one of the challenges of the eMobility developments.

2.1.4 The future of eMobility

The eMobility charging infrastructure will be available country and eventually EU-wide to allow vehicles to charge wherever and whenever they need to. The vision is that electric vehicles will be plugged into a charging spot whenever they are not driven. Hence, the battery is constantly charged, so that the batteries are always full enough for the next ride. The infrastructure has to be compatible with all electric vehicles. Compatibility relates to the charging plug, the communication and the billing process. Since the vehicle may be plugged-in to charge and unplugged multiple times a day, the charging process has to be simple and user-friendly. The idea is to automate the billing, so that the EV driver does not have to take any extra steps when leaving with her vehicle. Once plugged-in the charging spot the vehicle will handle the charging process and billing. This scenario is referred to as "plug-and-charge" [60]. The EV driver will have a contract with a mobility operator or her domestic utility company for charging the vehicle. The mobility operator will bill the EV driver for the charging expenses. Roaming should be possible when the vehicle is charged at a different provider than the one the driver has a mobility contract with. In the future charging may even be wireless and initiated by the vehicle itself, so that charging the vehicle is no different from parking it [83].

To make electric driving more attractive, automotive manufacturers propose new in-vehicle services. Via the vehicle-to-grid connection, the automotive manufacturers and other third parties can offer additional services, for example, remote diagnostics, navigation system updates and entertainment. Further, electric vehicles may offer benefits to the electricity grid. Use cases include, using the electric vehicles as energy buffer and to smooth out the electricity demand by instructing the vehicles to charge when the demand is lower [26].

The next step for eMobility is to provide a good coverage of charging stations and to align the efforts to one compatible infrastructure.

2.2 Infrastructure

This section explains the eMobility infrastructure and the involved stakeholders. Further, it gives a brief overview of relevant communication protocols.

The eMobility infrastructure comprises the electric vehicles, the charging stations, and the power grid. Also other parties that are not directly required in the charging procedure, such as the automotive manufacturers, maybe considered part of the eMobility infrastructure. The power grid and these additional parties are often referred to as the backend. The backend is required to handle the energy exchange, billing and additional services. The power grid can only communicate with the vehicles via

the charging station. The connection between the electric vehicle and the charging spot is called the vehicle-to-grid (V2G) interface.

The eMobility infrastructure allows bi-directional energy and data flows. The communication is transmitted via power-line-communication (PLC), the Internet and the cellular network. Open standards as well as special purpose protocols are used. An overview of relevant protocols is given in subsection 2.2.2 below. Figure 2.1 gives a high-level overview of the eMobility infrastructure.

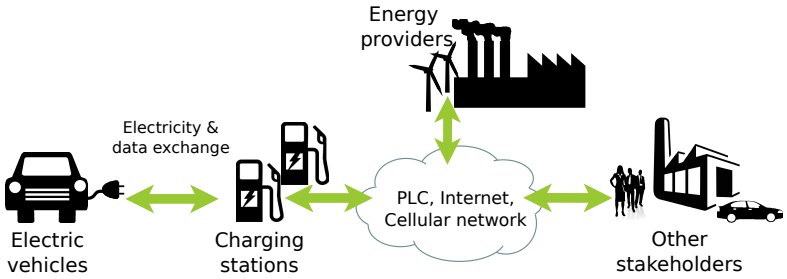

Figure 2.1: The eMobility infrastructure.

The electric vehicle plugs into the charging station. The communication goes via the power-line. The charging spot is connected to the power grid for the electricity delivery and communicates with the grid using PLC until a near by aggregator station and then the cellular network or the Internet. Multiple energy providers[1] are connected to the power grid.

Electric vehicles (EVs) eMobility in not limited to cars, but also includes other vehicles such as vans, buses, trucks motorcycles and scooters. The two main types of electric vehicles are fully electric vehicles (FEV), also called battery electric vehicles (BEV), which have no auxiliary on-board power. The other type of electric vehicles includes plug-in hybrid electric vehicles (PHEV) and extended range electric vehicles (EREV), which both have an internal combustion engine (ICE)) that recharges the battery and/or drives the wheels when the internal battery is used up.

The electric vehicles can go to any charging station to recharge the battery, i.e. all charging stations are technically compatible with all electric vehicles.

Charging stations There are several types of charging stations. Using a standard socket (16 Ampere and 230 Volts, i.e. 3.7 kW) it takes approximately 10 hours to charge an empty battery that has a range of about 150 km [53]. This means that a lot of vehicle owners may want to charge their car while it is parked somewhere for a longer period of time. This could be overnight while it is parked at home, during the day on the employer's or the shopping mall's parking lot and any other parking facilities. To quickly charge the e-vehicle special fast charging stations are required. These charging stations are similar to gas stations for fossil fuel powered vehicles. Stopping at such a station is an intentional stop for the purpose of charging in a short time [26]. Fast charging at 200 kW would take about 11 minutes for an empty 150 km range battery [53]. Currently, the highest power levels considered by the focus group on European eMobility are at 86 kW [26]. At this power level charging a 150 km range battery should take around 70 minutes. Table 2.1 summarizes the different charging locations.

Power grid The grid includes the electricity producers and distributors. The grid has a hierarchical structure, i.e., depending on the transmitted voltage the grid is divided into high, medium and low voltage grids. The power plants are connected to the high voltage grid. The low voltage grid supplies

[1] The terms energy provider and energy supplier are used interchangeably. An energy distributor is an intermediate of the energy infrastructure which manages the energy distribution between different voltage power grids and other grid sections. A distributor does not have to produce energy itself. Distributors are not considered as separate party in the eMobility infrastructure.

Location	Charging speed	Ownership	Energy supply
At home	Slow	Private	Domestic energy supplier, possibly separate charging connection/meter
At employer	Slow	Private	Employer's energy supplier, possibly separate charging connection/meter
Parking lot, e.g. shopping mall	Slow	Private	Parking lot operator, possibly separate charging connection/meter
Public parking	Slow	Municipality	Newly deployed connection
Fast charging station	Fast	Private	Newly deployed connection

Table 2.1: Charging station types ([26, 37])

electricity to residential areas and businesses [46]. Often the low voltage grid is divided into small sections called micro grids.

The power grid is monitored and managed by the advanced metering infrastructure (AMI). Smart meters monitor the electricity usage and report the consumed amount to the energy supplier in intervals of one hour or less [86]. This makes it possible to closely monitor the energy consumption and allows energy distributors to manage the electricity supply to smaller grids based on the real-time demand.

In order to significantly reduce the dependency on fossil fuels and nuclear power plants, more and more renewable energy sources are used. For energy providers renewable energy sources often pose challenges. Since the amount of electricity obtained from renewable sources can fluctuate a lot, the electricity amount is hard to predict and cannot be controlled. For example, solar power highly depends on the cloud coverage and can only be utilized during daytime. Similarly wind energy is weather dependent and exponentially increases until it reaches a certain wind speed. Once this ceiling value is reached any further increase in wind speed will not create more electricity [92].

Other stakeholders Vehicles manufacturers and other third parties are interested in making use of the V2G connection to offer additional services. These stakeholders are not directly required for the vehicle charging process.

All the stakeholders of eMobility are discussed next.

2.2.1 Stakeholders

The eMobility infrastructure knows several stakeholders that all want to contribute and benefit from the eMobility system. Here, we will briefly describe each of them, including what their input to eMobility is and what they expect to get in return and possible requirements. Figure 2.2 summarizes all the stakeholders.

Charging infrastructure The charging infrastructure includes the various types of charging stations and the power grid they are connected to. To offer fast charging new connections need to be installed. For slow charging the current infrastructure is sufficient [26, 53]. Beside the electricity exchange the charging infrastructure is also responsible to securely transmit any required data, such as billing information. Furthermore, all charging systems (i.e. plug, communication protocol) should be compatible with each other and any type of electric vehicle, so that vehicles can charge at any charging station. The charging stations are operated by an electricity supplier, similarly how gas stations are affiliated with an oil company.

Electrical vehicle owner/driver Most commonly the vehicle owner is also the vehicle driver, unless the vehicle is owned by a company, as in the case of company cars, fleet services, or rental vehicles.

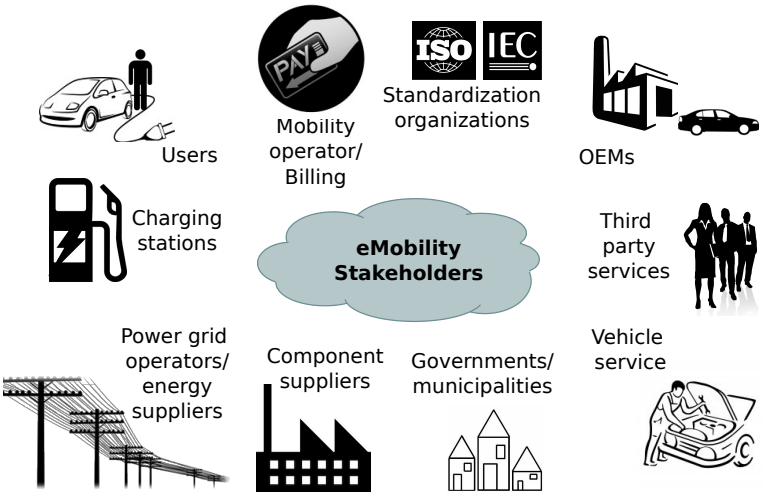

Figure 2.2: The stakeholders involved in eMobility.

The vehicle driver will want to have a similar (or better) experience as he is used to with combustion engine vehicles. The charging and billing process should be convenient and possibly quick [26]. The EV driver is often considered the user of the eMobility system.

Electricity companies Electricity companies include the energy suppliers and distributors. The increasingly interconnected energy grid allows more detailed and near real-time energy demand monitoring. The variable supply of renewable energy can be matched with the demand. Energy providers hope to store excess energy in electrical vehicles, and retrieve the energy when energy supply is low and the vehicles do not need the energy [92]. This is called smoothing out the energy demand. For example, on a bright, sunny day the energy provider may want to pass on all the energy to plugged in vehicles. The energy exchange needs to be closely monitored and the vehicle's bill is debited or credited accordingly.

Governments/municipalities, European Union Due to the environmental benefits, many governments are exploring the possibilities of electric driving. Studies are conducted how to increase the number of electric vehicles, what impact eMobility can have and how to support the trend [6, 49]. Further, governments and the European Union are aiming to align the eMobility efforts to produce an international, compatible infrastructure.

Mobility/Billing operator Several billing methods have been proposed. The main approaches are prepaid, subscriptions and billing via the domestic energy bill [86]. Mobility operators may offer contracts similar to mobile phone subscriptions with which the vehicle driver can charge at any associated charging stations. Also, roaming at other charging stations may be supported [103].

Standardization organizations The international standardization organizations, as well as workgroups formed by them and other stakeholders are currently investigating the eMobility opportunities [49, 51, 62]. The International Standards Organization (ISO), Society for Automobile Engineers (SAE) and International Electromechanical Commission (IEC) have released various standards regarding battery management, communication protocols and charging sockets/plugs [51]. Also, national organizations such as the Deutsches Institut für Normung e. V. (DIN) and the Japan Electric Vehicle Association Standards (JEVS) are offering standards.

The ISO/IEC 15118 standard (at the time of writing still under development) addresses the e-vehicle to grid communication interface, including use-cases, network and application protocol requirements and physical and data link layer requirements [51].

Third party services/Value-added services Several business models can be created for electric driving [103]. During the charging period additional content, such as location based advertisement and infotainment data, can be made available to the vehicle driver [92]. Also, short-term leasing of cars or car-sharing is a possibility, with charging station parking lots acting as pick-up stations [103].

Vehicle component suppliers Many vehicle component suppliers are joining the eMobility developments by delivering their own solutions for charging and charging interfaces [11, 13, 92]. Some component suppliers see themselves as possible charging equipment manufacturers and already offer charging stations for testing electric driving both as electric vehicle owner but also for potential charging station operators.

Vehicle manufacturers The electric vehicle (EV) itself is a very important asset in eMobility. Currently, only few electric vehicles are on the market and the incentives to purchase an EV are low [52]. However, vehicle manufacturers are planning to increase the supply of electric vehicles.

The vehicle manufactures Audi, BMW, Chrysler, Daimler, Ford, General Motors, Porsche and Volkswagen have agreed to use the same single-port fast charging approach. This approach is to be available in Europe and the United States. The first commercial fast-charging stations are expected to be functional by the end of 2013.

Further, the grid connection offers benefits for manufactures. While the vehicle is connected to the grid and likely to the Internet, the manufacturer can perform remote diagnostics and firmware upgrades.

Vehicle service stations Similarly to vehicle manufacturers service stations can make use of the possible "online state" of the vehicle and send diagnosis reports directly to the manufacturer for inspection.

2.2.2 Communication protocols

Communication is an essential part of vehicles of all kind, smart grids and electric vehicle charging. Compared to combustion engine vehicles, electric vehicles require additional communication to manage the energy flow to and from the battery while driving and for charging. Similarly, the power grid relies on accurate and timely communication with the connected smart meters. Vehicle-to-grid communication opens up a communication link between these two originally isolated environments, making security more important than before.

In the following, the relevant communication protocols used for electric vehicle charging and by the smart grid are described.

IEC 61851 – Electric vehicle conductive charging system

The IEC 61851 Electric vehicle conductive charging system series was standardized in 2001 and defines a conductive charging system. It addresses three modes for AC (alternating current) and one mode for DC (direct current) charging [26]. However, in only two of the four charging modes communication is takes place and no IT security is addressed [46]. AC charging is similar to charging at a conventional power socket and takes a long time. DC charging offers high voltages and low charging times, but needs to be monitored and regulated more strictly, so that the battery and the charging interface are not damaged [43].

ISO 15118 – Road vehicles: Vehicle to grid communication interface

To address the growing V2G communication and security requirements the ISO/IEC 15118 standard is being developed in Europe. In the USA, the V2G communication is addressed by the SAE J2836/2847 standard. The ISO/IEC 15118 standard proposes a communication protocol between

electric vehicles and the grid and addresses several use-cases, communication layers and their requirements. The focus of the protocol is on the electric vehicle to charging station connection using power-line communication. The communication with the backend infrastructure is not directly targeted and mostly left open. The standard also addresses the automated billing scenario. Security is a included as a requirement of the protocol and offers sufficient protections against most attacks described in [46]. However, user privacy is not discussed separately. The protocol assumes that the electric vehicle trusts the charging station – for privacy and insider attacks. A more detailed study of this vehicular charging protocol is given in Section 3.3 and 3.4.3.

IEC 62056 – DLMS/COSEM

The DLMS/COSEM standard is used in the smart grid for the data exchange with energy meters. A standard was required so that different energy companies have a common language for communication [38]. Several communication media are supported, such as PLC, GSM, GPRS and Ethernet. DLMS/COSEM is currently being finalized. The Device Language Message Specification (DLMS) defines the abstract concepts for the communication. The COmpanion Specification for Energy Metering (COSEM) specification defines the transport and application layer of the DLMS protocol. Together they are used for transporting information between metering equipment and the data collection system [38]. For example, the smart meters in domestic houses use DLMS/COSEM to communicate with the energy provider. Like the ISO standard, the COSEM standard equates privacy with confidentiality.

At the point of writing it is unclear how and if the eMobility system will make use of the DLMS/-COSEM standard for the backend communication. In the eMobility infrastructure DLMS/COSEM can be used by the charging station's smart meter to communicate the electricity requirements, negotiate the pricing and to report the actual electricity consumption back to the grid. Whether this protocol can also handle the automated billing is unclear.

IEC 61850 – Communication networks and systems in substations

The IEC 61850 standard originally was developed for automating substations. Substations are part of the energy network and fulfill roles such as transforming the power voltage from high to low or interconnecting different sections of the energy grid. During the last years IEC 61850 was adapted for the integration of distributed energy resources (DER) into communication networks. DERs generate electricity from many small energy sources, such as solar panels and wind power system, rather than a big power plant. In the future electric vehicles can function as DERs when they deliver energy back to the power grid. For managing this the IEC 61850 can be used [15, 85].

Several protocols for electric vehicles, smart grids and V2G exist. However, there is no end-to-end specification for a complete charging process and billing. For the charging communication between the electric vehicle and the charging station the ISO 15118 protocol will be used. But, to build an overall secure eMobility system, it is necessary to define how the charging and billing communication proceeds in the backend. Also, the security of the backend communication needs to be integrated with the security approach of the V2G communication. In relation to privacy, it remains unclear what data is transmitted into the backend and who will be able to read it.

2.3 eMobility & privacy

A lot of related technologies, such as smart metering or electronic payment, have been associated with privacy concerns. Smart metering can reveal behavioral patterns of the customer, for example, whether the customer is at home or sleeps late, because the frequently transmitted electricity readings [32, 68]. Similarly, electronic payments are mostly directly tied to the individual making the payment.

Electric vehicle charging makes use of smart meters and electronic payments. A smart meter is installed in the charging spot and communicates the electricity usage back to the grid. Electric vehicles will not have their own smart meter. Hence, the smart meter will likely not pose any privacy concerns. However, the payment requires billing data to be sent to the mobility operator, who has to identify which customer to bill and which electricity provider to pay for the charge. Also, for initiating the charging the electric vehicle may have to identify itself to the charging infrastructure. This identification most likely is unique.

The eMobility system is a large distributed infrastructure, that requires several messages to be exchanged. Table 2.2 gives a general overview of the messages. Some of the messages can contain sensitive information about the EV and hence the vehicle driver or other stakeholders. Privacy-sensitive data of the eMobility system includes customer data, charging location and time, billing details, as well as, third party data, e.g. firmware, that is transmitted via the charging spot.

Peer 1	Peer 2	Data exchanged
EV	Charging station (CS)	Charging control data, metering values, payment method, pricing
EV	Mobility plan operator (MO), e.g. EV's domestic utility company	Charging details (electricity amount and provider), EV authentication
EV	Vehicle manufacturer	Remote diagnostics, firmware upgrades
EV	Value-added-service provider	Other services (traffic, entertainment, etc.)
MO	CS	Payment method confirmation/authorization
CS	Energy provider	Charging details (electricity amount, location, pricing)
CS	MO	Billing details

Table 2.2: Possible EV communication relations and data exchanged [60].

Due to the short range and long charging duration, electrical vehicles should be plugged into a charging spot whenever they are parked. On average most vehicles remain parked 95% of the time in a day [108]. Therefore, an electric vehicle is constantly exchanging potentially sensitive data. For example, the charging locations may vary during the day, but will mostly include the driver's home and work. Recording the EV's location may reveal personal habits and information about the drivers' lives. As a future use case, grid operators consider using the batteries of electric vehicles as temporary energy buffers to store excess energy or to overcome a shortage of energy. This gives another reason why EVs should remain plugged in when they are not driven. For optimal monitoring and planning, grid operators are interested in near real-time information on EVs' charging battery status, locations and schedules, and may also require to know billing details.

The ISO 15118-1 document lists several payment methods, such as cash, prepaid, credit card and RFID card [60]. However, the method most concentrated on is contract based payment. In the eMobility system it will be common practice for the vehicle driver to enter into a billing contract with a mobility operator, or to add the charging expenses to the domestic energy bill [61, 103]. For maximum accountability the charging station and billing company will want to have all the data on the charging process (e.g. name, ID, location, amount).

In addition, to the potential privacy infringements of the eMobility system, working with personal data also requires adhering to the legal regulations of the European Union for the collection, storage, disclosure and use of personal data. This non-technical aspect also needs to be considered when designing the eMobility system.

Users of the eMobility system do not want their information to be transmitted to various parties, during 95% of the day. The privacy of the eMobility users should be protected by the design of the

eMobility infrastructure or other measures.

To overcome the privacy concerns for smart metering, privacy-preserving have been proposed [24, 25, 80]. Privacy-enhancing technologies (PETs) offer technical means to reduce the privacy impact of the technology. Another solution is to include privacy considerations already during the design phase of the technology. This approach is called "Privacy by Design". Similarly, privacy-preserving technologies are required to eliminate the privacy concerns of electric vehicle charging. Now, while the V2G protocols are still in development, privacy can still be included in the design of the protocols.

2.4 Challenges for eMobility

The eMobility industry faces several challenges, ranging from standardization to public acceptance of electric vehicles.

Though various organizations are developing charging solutions, including interfaces, communication protocols and network requirements, the result is a too large number of standards [51]. The vehicle manufacturers Audi, BMW, Chrysler, Daimler, Ford, General Motors, Porsche and Volkswagen have agreed to work together to support the same charging method [102].

Further, the common opinion about electric vehicles is that they have short ranges and are less powerful. Also, potential EV buyers are uncertain about the vehicle's durability and warranty. Currently, the purchase costs of an electric vehicles are higher than for a similar sized fossil fuel consuming vehicle [6], while the running costs are estimated to be significantly lower for electric vehicles [49]. There are few incentives to buy electric vehicles, hence slowing the deployment of eMobility [49]. The eMobility infrastructure is still under development, charging takes a long time and the currently available solutions are often not inter-operable. The necessary communication protocols are still being developed.

Finally, security and privacy aspects are rarely addressed. Security is mainly considered to prevent the vehicle from cheating the system, however malfunctioning charging stations, cheating billing operators or other attacks are not addressed. Also, what impact eMobility will have on the driver's privacy is unclear.

2.5 Focus of the thesis

Security aspects for the communication protocols, smart grids and electric vehicles, as wel as, privacy for smart metering has been studied [33, 42, 47, 74]. However, the privacy impact of electric vehicle charging is largely unknown. This thesis investigates the privacy impact of electric vehicle charging and proposes a technological approach to make charging privacy-preserving. The focus is on the eMobility user's privacy in the plug-and-charge with contract-based payment usecase. The privacy analysis mainly considers private individuals rather than fleet operators, since private destinations are more sensitive than fleet destinations. The ISO 15118 standard will be used as a basis for this discussion whenever possible. Given the current developments, this standard is most likely to be implemented in practice. Any assumptions or alterations of existing systems will be kept as minimal and realistic as possible. The proposed protocol addresses the information flows; the monetary flows are secondary to this solution.

CHAPTER 3
The eMobility infrastructure

At the moment, the eMobility infrastructure is only partially defined. The charging communication between the vehicle and the charging station is described in the ISO 15118 protocol. However, the backend communication of the eMobility system is left unclear. This chapter analyzes the eMobility system requirements and the architecture for the contract-based payment charging usecase. Next, the ISO 15118 charging protocol is analyzed in detail, including its security and privacy approach.

3.1 eMobility requirements

The eMobility requirements can be split into two groups based on which stakeholder's perspective is used. We will focus on the users' and the overall system requirements.

Requirements – User perspective This perspective focuses on the eMobility users, i.e., the EV drivers that will be making use of the charging system. These requirements are based on reports and recommendations for eMobility, such as [26, 49, 84, 106].

The future EV drivers are likely to be used to combustion engine vehicles and expect a similar or better experience when driving, recharging and servicing their vehicle. Also, it should not be expected that the EV driver will want to do extra actions for an electric vehicle. Especially, standard (slow) methods of charging, which may be initiated multiple times a day, should be convenient and simple. The user's system requirements have been summarized below:

U1. Charging system has to be user friendly and convenient. The charging setup should be simple and understandable for current combustion engine drivers. It should not require technical knowledge.
U2. Charging should require little/no interaction, i.e., it should be automated and handled by the vehicle and the charging station.
U3. Convenient payment methods, such as grouping of charging bills, since the EV is charged multiple times a day. A solution is to automatically deduct the expenses of the bank account or add them to the domestic energy bill.
U4. Users should be able to roam, i.e., charge at any charging station no matter what charging contract the EV has or in which (European) country the vehicle is trying to charge.

In addition, to these requirements there exist privacy-related requirements. The privacy of the EV user should be preserved. As discussed in Section 2.3, the charging location can reveal where the vehicle has been, e.g. if a local energy provider is used. Similarly, a local mobility operator can reveal where the EV user lives, since it is likely to the same provider as the domestic energy provider. Hence, the identity of these parties should be hidden from each other. This privacy requirement can be summarized as:

P1. None of the stakeholders should be able to track EVs (and hence eMobility users) or obtain other private information during a charging process. This is the privacy requirement.

Requirements – Overall system perspective The overall system requirements are those that decide how feasible the charging system is. A user-friendly and simple charging system may not be workable for the power grid or energy companies, for example, because it requires too much new infrastructure or new parties for management and control. These requirements are based on infrastructure studies and reports, such as [14, 53, 106].

The overall requirements have been summarized below:

S1. The system should require the least (new) changes to the current power and IT infrastructure.
S2. The system should not rely on third parties if it can be avoided.
S3. The EU's legal (privacy) regulations have to be fulfilled.
S4. Trust cannot be assumed between the stakeholders and participants of the system.
S5. Authentication may be required for charging.
S6. Accountability is important for billing.
S7. Cheating of the system should be impossible or at least made infeasible.

It should be noted that whether or not the requirements are fulfilled by the eMobility infrastructure depends on the complete implementation, not only the communication protocols.

3.2 The charging architecture

Next, we discuss the charging architecture based on the description the ISO/IEC 15118 protocol [60, 61]. At the time of writing, the ISO/IEC 15118 protocol is in the final phase of being standardized and is likely to be adopted as the European charging protocol. The ISO 15118 standard's main purpose is to define the electric vehicle charging communication. It also offers possibilities to support additional functions, such as in-vehicle Internet access and OEM vehicle access [60]. Several payment methods are possible, for example, using a prepaid card, credit card or bank account. However, these payment methods are external mechanisms and require user interaction. The focus of the standard is on contract-based payments which are initiated and completely handled by the vehicle. Automated contract-based payment matches the users' requirement for a simple and convenient payment method.

The contract-based payment scenario is often referred to as "plug-and-charge" [60] or charging with automated payment. To charge the electric vehicle (EV) is plugged into the charging station (CS), e.g., on a public parking lot. The charging station is operator or associated with an electricity provider. This provider delivers the electricity and receives the payment for the charging expenses. The charging station and the electricity provider can communicate via the charging station's smart meter and other communication interfaces using the power grid, cellular network and/or the Internet.

In order to automate the billing, the EV's owner enters into an mobility contract with a mobility operator.

The mobility operator might be the same as the operator of the charging station, another energy provider or a third party [60]. Often the mobility operator will be the same energy provider as the EV owner's domestic energy supplier. In all cases the EV can charge at the charging station. If the charging station's energy provider and the mobility operator are not the same company the EV is said to be roaming. Some mobility operators may charge roaming fees or offer other special tariffs as agreed in the mobility contract [60]. The mobility operator obtains the charging bills in the form of service detail records (SDRs) from the charging station or an intermediate clearing house and pays the respective energy providers. The SRDs contain all the necessary information that the mobility operator needs for billing and informing the EV user for the charging session [60].

The ISO 15118 standard refers to the electric vehicle and the electric vehicle as the primary actors. All other actors are called the secondary actors and form the backend. The standard also describes one or more clearing houses that may be used to support the backend communication by forwarding messages to the correct party or distributing required certificates. For example, a clearing house may be used to obtain or update any of the EV's certificates. The standard keeps the descriptions of the

communication with and within the backend vague, so that the backend cannot be clearly defined based on ISO 15118 alone.

The electric vehicle, the charging station and the backend form the charging infrastructure. The backend consists of the CS's energy provider, the EV's mobility operator and possibly one a clearing house. The architecture is depicted in Fig. 3.1.

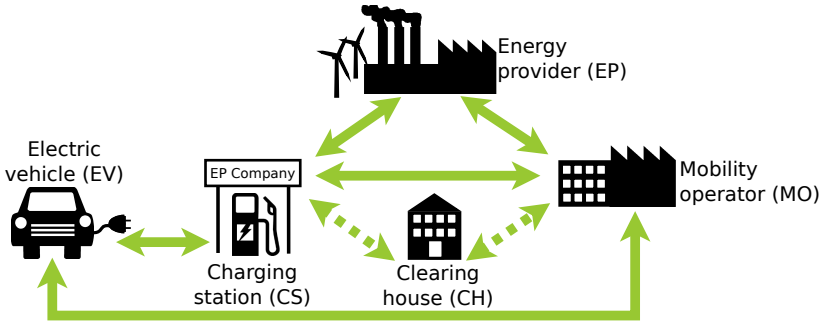

Figure 3.1: The information flow between the stakeholders in the plug-and-charge usecase.

A few open issues remain when considering EV ownership and contract sharing. The ISO standard suggests that a charging contract is linked to an EV, thereby allowing multiple drivers to use the vehicle while sharing the charging expenses. However, this may be problematic in case of rental vehicles. Further, it is unclear who is liable to pay the charging bills – the EV user or the MO. These issues cannot be solved technically.

3.3 The charging protocol

ISO/IEC 15118 is divided in three parts. ISO/IEC 15118-1 describes general information and use-cases at application level. Part 3 addresses the physical and data link layer requirements. ISO/IEC 15118-1 and 15118-2 are the most relevant for this study. Part 2 provides the technical protocol and OSI (Open System Interconnection) layer requirements and it describes the application level protocol used for the communication between the EV and the EVSE (electric vehicle supply equipment), i.e., the charging station. This section discusses the messages exchanged when charging with contract-based payment.

On the EV's side the communication is managed by the electric vehicle communication controller (EVCC). On the grid's side the supply equipment communication controller (SECC) manages the communication. The communication follows a client-server approach, where the EV is the client and the charging spot (CS) is the server.[1] Figure 3.2 illustrates this communication setup.

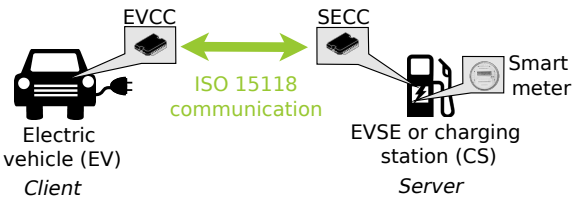

Figure 3.2: The ISO 15118 setup.

The ISO/IEC 15118 protocol is initiated as soon as the electric vehicle is connected to the charging station. Before the high-level communication starts the physical and data link layers connection is established (specified in ISO/IEC 15118-3). The vehicle obtains an IP address by issuing a DHCP

[1] For simplicity, we will ignore the distinctions between the electric vehicle and EVCC, and equally the EVSE and SECC. We will refer to two the two communicating parties as the electric vehicle (EV) and the charging station (CS).

request and runs the discovery protocol to find the IP address and port of the charging station. Finally, the electric vehicle and the charging station agree on the application-level protocol version. Now the application level ISO/IEC 15118-2 protocol starts.

Figure 3.3 gives a high-level overview of the messages exchanged between the electric vehicle and the charging station during a contract based charging process.

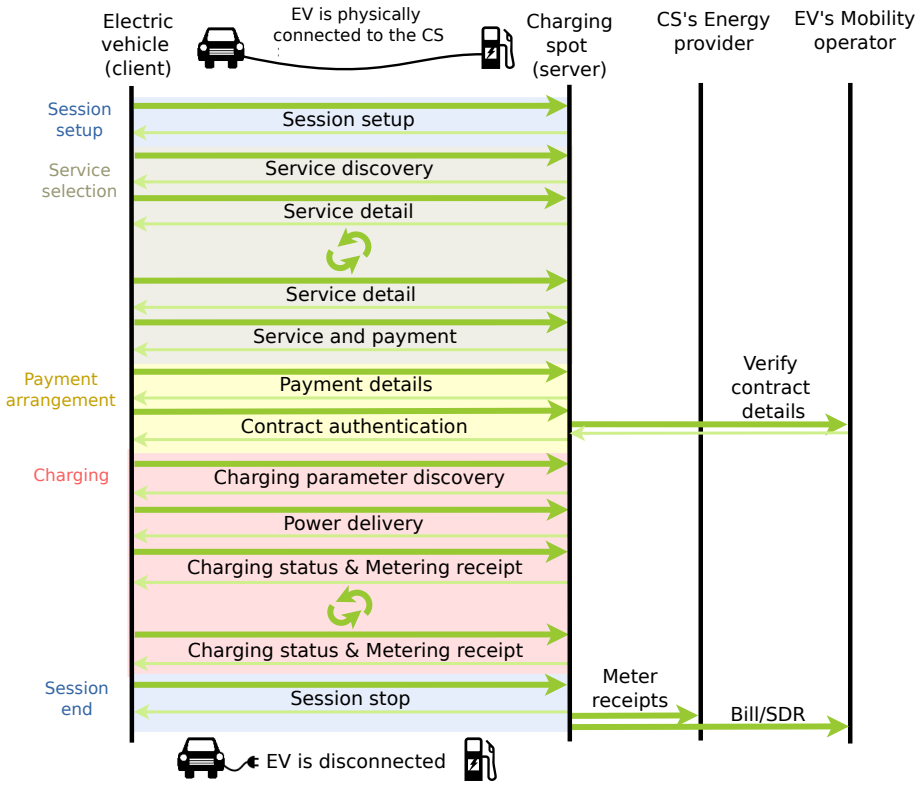

Figure 3.3: Communication between the EV and CS according to ISO/IEC 15118-2 using a contract based payment.

First, the *session* is *initiated* and the electric vehicle and charging station identifiers are exchanged, i.e. the EVCCID and the EVSEID, respectively. Then a unique session ID is selected, which is to be used for the complete communication process. Next, the *service discovery* takes place. The vehicle queries the charging station to find out which services the charging station can offer, e.g., charging and payment modes, Internet access or other value added services. The ISO standard only addresses services related to charging, but indicates that additional services can be integrated with the protocol at this point. The charging station responds with the list of available services. The vehicle can request additional information on a specific service by sending a *service detail request*.

Then, the vehicle performs the *service and payment request* and the payment details are sent to the charging station. In the case of contract based charging, the EV's charging contract identifier (*ContractID*) and the corresponding contract certificate is sent to the charging station as part of a *contract authentication request*. Then the charging station informs the vehicle whether the payment details have been accepted. If accepted, the vehicle can start charging at the charging station.

Next, the charging parameters are negotiated using a *charging parameter discovery*. The vehicle provides the charging station with status information on the vehicle/battery and other parameters, such as an estimate of the required energy amount and prospective end time of the charging process, i.e., when the electric vehicle wishes to disconnect from the charging station. In return the charging station informs the vehicle about applicable grid parameters for charging, tariffs and other costs, based on which the electric vehicle may optimize its charging process. At this point it is also decided

whether AC or DC charging is to be used.

Then, the *power delivery* starts with the charging station enabling the energy flow to the vehicle based on the charging profile of the electric vehicle. Depending on the charging method selected, additional method-specific messages may be exchanged, e.g., to perform a cable check, welding check or to set the current demand. During the charging loop *charging status* messages are exchanged. The charging station sends its status message together with the current meter readings that indicate the amount of energy consumed by the vehicle. For reliable billing the charging station asks the vehicle to sign these meter readings as a proof. The vehicle can perform a plausibility check to compare the received and delivered energy amount. The vehicle sends the signed meter readings and its own status back to the charging station. In addition, these messages are used to keep the communication session alive. The charging station may send the signed meter readouts to the mobility operator for billing. By sending a *session stop request* the vehicle asks the charging station to terminate the charging process.

The standard allows online and semi-online (also referred to as offline) charging spots. In most cases it is required that the charging station is online at least once a day. In this context, "online" means that communication with the backend (e.g., energy provider, mobility operator) is possible. An semi-online connection is required to communicate back the energy consumption (e.g., signed meter readings) and to be informed about certificate revocations. A real-time online connection is necessary to update EV and CS certificates. The standard requests that charging stations that cannot support online functions should be physically labeled as "offline EVSE" or similar. Further, the ISO/IEC 15118 standard also considers private charging spots at the EV user's home which will always be offline. The standard argues that the same charging protocol can be used. No communication with the backend is required, because the electricity consumption is automatically recorded by the domestic energy supplier.

3.4 Security & privacy

The ISO/IEC protocol considers security to be an important aspect in vehicle charging. High voltages are transferred during the charging process and tampering with the charging communication may damage the battery, electronic equipment or injure the user. Further, the electricity has to be paid for. Hence, the protocol has to be robust and secure. For example, if the charging cable is unplugged before the charging process completed, the electricity supply has to be stopped and the amount of electricity consumed up to that moment has to be paid. The eMobility system requirements have been discussed in Section 3.1. Points 4 to 7 of the system perspective are security-related requirements. These requirements can be split into the general security goals: confidentiality, data integrity, authentication, non-repudiation as well as reliability/availability.

First, this section discusses the security requirements. Then, it describes possible attacks and explains what security measures the ISO/IEC protocol integrates in the charging communication discussed in the previous section. Finally, the privacy requirement (see Sect. 3.1 user perspective) and the standard's approach is examined.

3.4.1 Security requirements

Each requirement is analyzed with respect to the eMobility architecture and charging scenario discussed above.

Confidentiality By default all data should be kept secret from all parties except those that are authorized to have it. During the V2G connection information is exchanged between the electric vehicle, the charging station and other parties in the backend. For charging it is usually necessary to send vehicle and contract identifiers and payment details. This is sensitive information and could be abused for attacks. The possible communication relations and the data exchanged are summarized

in Table 2.2. Further, certificates and keys may be stored inside the vehicle and the charging station to encrypt or sign messages. This data also has to be protected.

Integrity It is viable for the eMobility system that unauthorized manipulation of any data is impossible or at least detectable, for example using checksums. Data alteration includes insertion, deletion and substitution of the actual data with other values. During the charging process metering values, charging parameters and contract identifiers are exchanged. Further, the eMobility system wants to offer software and firmware updates while the vehicle is charging. Modification of such data can cause damage to the vehicle or the charging station, for example if the maximum allowed voltage is increased or the firmware is modified. Hence, data stored locally or transmitted has to be integrity-protected.

The integrity requirement can be extended to important eMobility components, such as the energy meter and the charging station. Tampering with this equipment should be impossible or at least detectable.

Authentication It is important that all communicating parties identify each other before exchanging any information. The electric vehicle and the charging station should authenticate each other to be certain they are communicating with a genuine counterpart. Each party could posses a certificate to authenticate itself. More importantly, the vehicle has to be authenticated for payment at the charging station. The vehicle could show a proof which confirms that the vehicle has a charging contract. In addition, only authenticated parties should be allowed to communicate with the energy grid, because misuse may severely affect the power grid's operation. Hence, also the charging station has to authenticate to the grid.

Similarly, the origin, timestamp and data content of all transmitted data should be authenticated. For example, the charging station has to be sure that it is receiving the charging profile from the same vehicle, that also initiated the payment. Authenticating the data also provides integrity.

Non-repudiation The eMobility system should be accountable, i.e. all transactions should be logged and signed, so that no party can deny any previous actions. For example, while charging the charing station can require the vehicle to sign the meter reading every few kWs of received energy. The charging station can use the signature as proof in case the vehicle refuses to pay for the full amount of energy consumed.

Non-repudiation can also be provided by involving a trusted third party to witness the actions and resolve any dispute.

Reliability/availability Charging should be possible at any point of time. Usually, the charging station needs to communicate with the backend (i.e., energy provider, mobility operator) to authenticate the charging process and arrange the payment. If this communication is (temporarily) not possible the system should still keep working reliably. If the other security requirements are fulfilled it may be possible to perform the required data exchange at a later point in time. For example, the vehicle can present a proof that it will pay and signs the meter readings for the received energy. The charging station can then verify the payment data at a later point in time, since it can otherwise identify the vehicle that charged using the signature. Further, the system has to be reliable also in case of exceptions and should handle these correctly.

Falk and Fries identify similar security requirements in [46]. In addition, they suggest that the attack effect should be limited geographically and functionally. All control actions on the smart grid should be authorized, security relevant events are to be logged, and adequate security failure and exception handling is to be used. Finally, Falk and Fries note that standardization of the overall system including the security approach is necessary, because several different peers interact with each other, often using different equipment and vendors [46]. Only if the security approach is included in the standardization an overall, secure and reliable eMobility system can be developed.

The ISO 15118-1 document addresses which security requirements have to be fulfilled for which communication exchange (Table B.1 [60]) and for which data/service (Table B.6 [60]). The ISO 15118 standard divides the security requirements into accountability, authenticity, confidentiality & privacy, integrity, and reliability & availability. Table B.1 of ISO 15118-1 states, for example, that for simple charging communication authenticity, integrity, and reliability & availability is required. For charging with exchange of meter information also accountability and confidentiality is necessary. Based on Table B.6, billing information has to be integrity and non-repudiation protected and should be confidential if personalized. Software updates are considered OEM specific, but the standard proposes integrity and confidentiality protection. For charging control data integrity and availability are important. Overall, the ISO 15118-1 security suggestions match our requirements analysis.

3.4.2 Potential attacks

Falk and Fries discuss five potential threats [46]:

1. Eavesdropping or interception
2. Man-in-the-Middle attack
3. Transaction falsifying or repudiation
4. Tampered or substituted component
5. Attack network from within the vehicle.

Eavesdropping can be used to gain information without authorization. The data could be used to plan further, active attacks. For example, an attacker can listen in on the communication between the electric vehicle and the charging spot and learn the contract identifier of the vehicle. The attacker could then use the contract identifier when she charges her own electric vehicle. Similarly, an attacker could listen in on commands between the charging station and the power grid, and learn the commands used to operate the power grid. To protect against eavesdropping the confidentiality requirements has to be fulfilled.

During a man-in-the-middle attack an attacker intercepts the communication and modifies it before sending it to the original destination. Falk and Fries describe a man-in-the-middle attack between an electric vehicle and a charging spot. First, a fake charging spot tricks an honest customer to connect to it [46]. The fake charging spot then forwards the communication to the real charging spot where the attacker has connected her vehicle. The real charging station will see the payment information coming in from the honest customer and allow the electricity flow. The attacker then uses all or a portion of the delivered energy to recharge her vehicle, while the honest customer pays for all of the electricity. A man-in-the-middle attack could also be performed between the charging station and the grid. For example, an attacker may impersonate the mobility operator who receives the bill for the charging process and modify the amount payable before forwarding it to the real mobility operator. The integrity and authentication requirement have to be fulfilled to protect against man-in-the-middle attacks.

A customer may falsify information or deny actions. This could be done intentionally, as in the case of the man-in-the-middle attack, or unintentionally, due to malfunctioning equipment. Data integrity, authentication and non-repudiation can prevent this. For example, an attacker can modify the energy meter reading before sending it to the charging station. Similarly, an attacker can manipulate a component that is trusted by the system, such as an electricity meter or an on-board unit that regulates the charging communication and payment. An attacker could change the vehicle or contract identifier, so that someone else is charged for the energy expenses. Therefore, all equipment should be tamper-proof and integrity-protected.

Finally, an attacker could intentionally or unintentionally, because of software fault, attack the eMobility infrastructure from within the vehicle, for example, by injecting malformed data packets or overloading the system with requests. Such attacks can cause the system, e.g. the charging spot, to crash hence denying service. This attack affects the integrity and availability of the eMobility system.

Falk and Fries do not directly address attacks from within the eMobility infrastructure on the electric vehicle. However, a manipulated firmware update can have safety critical effects on the vehicle's functioning.

3.4.3 ISO/IEC 15118 security approach

Figure 3.4 illustrates the security communication of the ISO/IEC 15118-2 protocol for the contract-based payment scenario described in 3.3.

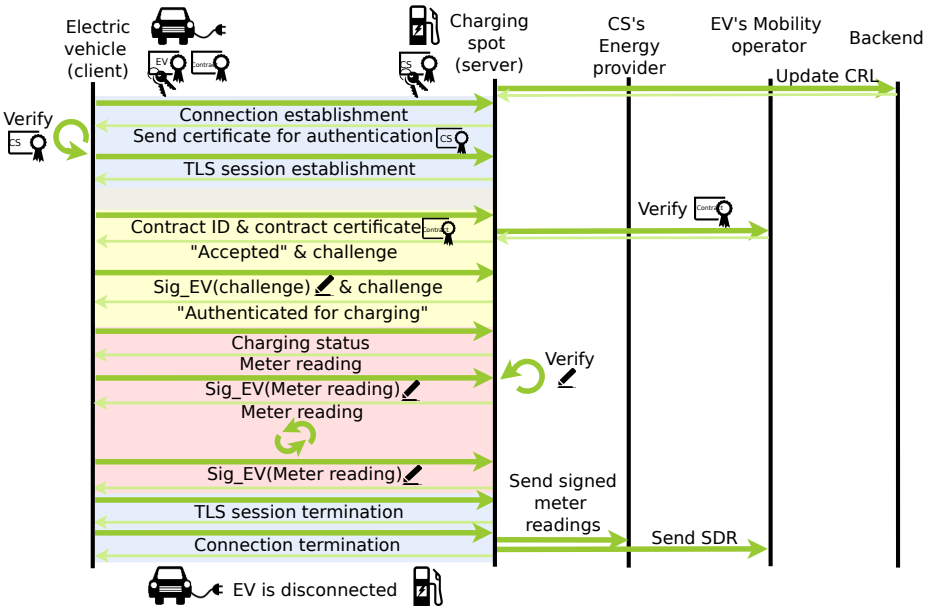

Figure 3.4: Security-related communication between the EV and CS according ISO/IEC 15118.

The standard [61] states that TLS (Transport Layer Security) is to be used at the transport layer to enable an authenticated and encrypted channel between the electric vehicle and the charging station. The authentication is unilateral, i.e. the charging station authenticates towards the electric vehicle. The unilateral authentication is mandatory and based on asymmetric long term key material. The standard notes that the charging station cannot check if the EVCC it communicates with is authentic, but gives no further reason why choosing this unilateral approach. The charging station possesses an identity certificate and a corresponding private key. The electric vehicle has access to the root certificate to check the authenticity of the charging sport's certificate. Both parties support CRL (Certificate Revocation List) or OCSP (Online Certificate Status Protocol) messages to check the validation state of certificates.

The presentation layer of the ISO 15118-2 protocol uses XML data representation with type aware XML Schema and EXI (Efficient XML Interchange) for encoding. XML security is implemented using XML Encryption and XML Signatures, to meet the security requirements of sensitive V2G data. XML security enables integrity, confidentiality and authentication of XML-based messages. XML signatures are used to protect the payment details provided by the electric vehicle to the backend. The receiving party will know who the sender is and the data is integrity protected. Based on the assumption that all communication between the electric vehicle and the charging spot is protected by TLS, only specific messages are protected at the application layer. XML encryption is used to protect sensitive data, so that no intermediaries can access the data when it is transferred by the charging station to the receiving party in the backend. Since the information intended for the backend is also encoded using XML data structures, the data can be protected end-to-end using XML security. While the channel between the electric vehicle and the charging station is TLS-protected at the transport layer to prevent eavesdropping, it is outside the scope of the ISO/IEC 15118 standard what additional (transport layer) security is used for communication with the backend. This will depend on the backend communication protocol, e.g., DLMS/COSEM.

Further, the ISO/IEC 15118 standard assumes that the electric vehicle only signs and the charging

station only encrypts data. A possible reason for this assumption is that not encrypting on the vehicle's side reduces the computing power requirements of the electric vehicle. Also, the electric vehicle has to sign messages as a form of proof; the charging station may sign messages as source authentication, but it is not mandatory.

The electric vehicle and the charging station posses asymmetric key material, i.e. a certificate and a private key. For contract-based payments, the vehicle's certificate/private key should bind a valid payment contract, i.e. a contract identifier, to a specific vehicle. First, the electric vehicle sends the contract identifier and contract certificate to the charging station (see "Payment arrangement" in Fig. 3.4). When the charging station informs the electric vehicle whether the payment details have been accepted the charging station includes a random number which has to be signed by the vehicle as a challenge. The electric vehicle sends the signature and the challenge back to the charging station. Then the contract certificate and challenge signature are verified by the charging station and if valid the vehicle is authorized for charging. Both parties have access to the root certificates to check the validity of certificates. Therefore, the charging station can also check the validity in offline charging scenarios. If the charging station is online it will directly contact the backend to verify the contract details. Figure 3.5 summarizes the certificates and how they are linked to each other.

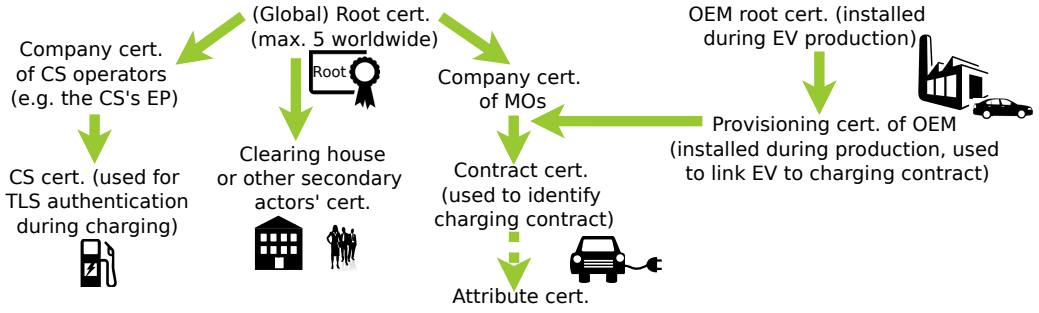

Figure 3.5: The ISO 15118 certificates.

For most protocol requests (e.g., *service discovery*) it is required that vehicle identification, authentication and authorization takes place. To do so the vehicle sends its *contract ID* and possibly also the *(mobility) provider ID* to the charging station. The charging station sends its *spot operator ID* and *Power Outlet ID* to the vehicle. When the charging station is online the validation can be performed in real-time. The charging station will forward the vehicle's identifiers and its own identifiers to the backend, and wait for a validation accept/decline reply [60]. In this case the Contract ID is used for identification and authorization. The ISO/IEC 15118 standard also suggests that other means of identification could be used, but they will require user interaction, e.g., to enter a PIN or password.

During the charging process the charging station sends the meter readings via the TLS-protected tunnel to the vehicle. A signature of the charging station is optional and can be included as source authentication. The vehicle sends the signed readings back to the charging station. This process is repeated multiple times during the charging process using the cumulated meter reading each time. The standard states that if the vehicle pays the charging station directly, the meter readings are deleted. For contract based payment the signed meter readings are stored and send to the backend (e.g., the mobility operator) when the charging station is online.

The standard proposes to use elliptic curve cryptography (ECC) for authentication and digital signatures because of the memory and computing power constrained electric control units used in vehicles and charging spots [46].

Based on this information the ISO 15118-2 protocol is secured against most of the attacks found by Falk and Fries [46]. Table 3.1 summarizes the attacks and the ISO 15118 security approach. The communication between the electric vehicle and the charging spot is protected by TLS and hence

protected against eavesdropping. Since the charging station authenticates itself towards the vehicle, a man-in-the-middle attack requires the attacker to have access to a valid certificate. However, it may be possible to perform the man-in-the-middle attack described by Falk and Fries, if the attacker only consumes a small amount of the energy and forwards all communication between the charging station and the victim's electric vehicle. Depending on how much energy is consumed by the attacker the charging station and the victim's vehicle may be able to notice a difference in the meter readings and abort the charging. The ISO 15118 protocol has some protection against transaction falsifying or repudiation by requiring the vehicle to sign the cumulative meter readings. However, the charging station may send a wrong meter reading. A signature of the charging station is not mandatory in the ISO 15118 standard. Tampered or substituted components are not detected unless a certificate/signature can reveal that the vehicle's identifier or other identifying data changed. This attack should be prevented by other means, e.g. tamper-proof hardware and integrity protected software and key storage. Data sent to the backend is protected by XML security. The ISO 15118 protocol states that billing information is integrity protected (XML signatures) and sensitive data is XML encrypted. However, it is not clear what is considered sensitive data. Assuming that all data is protected, interception between the charging station and the backend is infeasible. However, it is not clear how the charging spot will respond to attacks from within the vehicle. The protocol implements some error handling, so that the charging spot responds with a fault notification, for example, in the case of parsing errors or other decoding errors.

Attack	**ISO security approach**
Eavesdropping or interception	TLS for communication between EV and CS.
Man-in-the-Middle attack	CS authentication; MITM may be possible for stealing small amounts of electricity.
Transaction falsifying or repudiation	EV signs cumulative meter readings; CS signature not mandatory.
Tampered or substituted component	No protection unless certificate/signature can reveal the attack; other means are needed, e.g. tamper-proof hardware.
Attack network from within the vehicle	XML security for backend communication. Unclear how CS/backend will respond to crafted attack.

Table 3.1: Attacks and ISO 15118-2 security solution [46, 61]

The ISO 15118 standard addresses security, which offers sufficient protections against most attacks, but ignores insider attacks, e.g., from the charging station. Also, to build an overall secure eMobility system, it is necessary to define how the communication proceeds after the charging station and to integrate the security of the backend communication with the security approach of the V2G communication.

3.4.4 ISO/IEC 15118 and privacy

While the ISO 15118 protocol gives attention to security requirements it does not address privacy on its own. Privacy is mainly equated with the security requirement "confidentiality" [60]. However, part 1 of the standard states that private information and user data should only be readable by the intended addressed and is only transferred if necessary [60]. For the rest confidentiality is offered for the communication between the electric vehicle and the charging station and data sent to the backend is encrypted with at the application level with XML security mechanisms so that only the intended parties can view the data. It is not clear in the standard which parties, referred to as secondary actors, receive the data.

Further, some of the standard's procedures may lead to privacy concerns. Each vehicle posses a unique *Provisioning Certificate* with a *Cert ID* that is installed in the vehicle by the OEM during

the manufacturing process of the vehicle. The vehicle owner uses the identifier to get a mobility contract. The CertID links the vehicle to the charging contract. The vehicle can proof that it has a valid charging contract with the received contract certificate and the *Contract ID*. This identifier is used to authenticate the vehicle to the power grid when it requests to charge. As described above (see 3.4.3), the Contract ID is transmitted to the charging station for authentication when using contract-based payment. The may be sent into the backend together with the charging station's identifier to check the validity of the contract [61]. Due to the way the Contract ID is generated this identifier uniquely identifies a vehicle. Similarly, at the transport layer of the charging protocol an identifier that contains the MAC address of the vehicle is used for the session setup [61]. Anybody receiving the Contract ID or the MAC may be able to generate records when and where the vehicle has been charging. In general, the standard assumes that the charging station is a trusted by the electric vehicle. However, no direct personal information is sent in plaintext to the charting station [60]. The privacy impact of the ISO protocol will be analyzed using a Privacy Impact Assessment in Section 4.3.

3.5 Summary

This chapter has analyzed the eMobility infrastructure, including the system requirements, the architecture and the charging protocol. The messages exchanged according to ISO when charging with contract-based payment have been examined in detail. Further, the security and privacy approach of the ISO/IEC 15118 has been analyzed. The standard addresses security in the requirements and integrates it into the protocol. The protocol is secure against the threats found by Falk and Fries. Therefore, we will not look at further attacks or weaknesses in the protocol. However, it is evident that privacy was not a design goal. The privacy impact of the protocol is analyzed in the next chapter.

CHAPTER 4
Privacy in eMobility

This chapter investigates the privacy impact of electric vehicle charging. First, an introduction to information privacy is given. Based on the legal regulations and known privacy principles the privacy requirements for the eMobility system are determined. Next, privacy impact assessments (PIAs) are discussed and an approach for eMobility is worked out. Finally, the PIA is applied to the eMobility system and constructive suggestions are made for reducing the privacy-impact.

As stated in Section 2.5, this thesis focuses on the vehicle driver's (information) privacy[1] and the automated billing scenario for the privacy analysis.

4.1 Privacy overview

Privacy is one of the fundamental rights according to the United Nations Universal Declaration of Human Rights and other national human rights laws. However, the perceptions of privacy have changed over the years. Especially with the rise of information technology, which has simplified the collection and processing of information.

Several definitions of privacy exist depending on the context, country and culture [90, 91]. According to Warren and Brandeis privacy is "*the right to be left alone*" [104]. Nissenbaum's theory of "*contextual integrity*" states that a privacy violation occurs only in case of inappropriate decontextualization of private information, i.e. if private information was collected under certain conditions and the information is used otherwise [71]. Westin defines privacy as "*the claim of individuals, groups and institutions to determine for themselves when, how and to what extend information about them is communicated to others.*" [105]. This form of privacy is often refereed to as information privacy. For this analysis information privacy is the most relevant. Information privacy considers the collection, processing and storage of personal information[2] Personal information is data that can uniquely identify an individual. It is not necessary that an individual is directly identified, for example, by name, address or identification number. Data that indirectly identifies an individual, e.g., by means of data-mining, also is considered to be personal data [87, 99]. Indirect personal data is also called *personally identifiable information* (PII) [99].

4.1.1 Privacy requirements

When developing a system the privacy regulations such as the European Data Protection Directives EC/95/46 [45] and 2002/58/EC [44], or the U.S. federal privacy laws have to be taken into account [48]. These laws state under what condition personal data is allowed to be used and how it has to be handled. The Organization for Economic Cooperation and Development (OECD) has summarized the privacy laws in a list of eight key privacy principles in [73]. These principles are often used as the basis for privacy requirements. For this thesis we will focus on the European regulations.

[1] In this thesis no distinction is made between the vehicle driver and the vehicle owner unless otherwise stated.

[2] Personal information is also referred to as personal data, since often digital forms of collection/storage are used. The terms are used interchangeably.

Similar to the OECD privacy principals, Agrawal et al have created a set of ten principles for the design of hippocratic databases [2]. Despite being originally proposed for database systems, the principles have been successfully adapted for other domains, such as car-to-car communication [63]. Hence, we base our discussion of privacy requirements on an adaptation of Agrawal's principles. These principals are in line with the EU regulations for data protection and ePrivacy (cf. [44]). Privacy is considered from the point of view of the vehicle driver.

1) Purpose specification There should be a purpose for each data item that is collected. This purpose should be explicitly specified for reference. For example, a name, contract identifier and billing address may be required for handing the billing. Then billing is the purpose of collecting the data This is one of the EU data protection requirements.

2) Consent The driver should be informed about how her data is to be used and give her consent. For example, if the driver does not want her billing details to be used, the system should not offer such payment options to this specific driver. Instead she may be able to pay with cash or an anonymous prepaid card. Consent is one of the EU data protection requirements.

3) Limited collection Only the data that is required for system operation should be recored. For example, if it is not necessary to record the exact location of the charging station it should not be stored. Reducing the amount of collected data will also require less resources to protect the data.

4) Limited use When using a data item, e.g., a billing address, for some operation, such as sending a bill, this operation should match the purpose specification for that data item. For example, if a party wants to use the billing address of a user for targeted advertisement, but the purpose specification of the data item indicates that is it intended for billing only, the party may not use the data even if it has access to the data.

5) Limited disclosure Data should only be available to those parties that require the data and for whom the data subject has given her consent. If the user allowed gave her credit card number to the charging station, it should not be forwarded to a third-party that is not involved in the transaction.

6) Limited retention Data should also be stored as long as is required to finish an action for which the data has been collected. For example, the ISO 15118 standard proposes that if a user directly pays the charging station all meter data and other records on the transaction are deleted and not transferred to any third-party. However, there may be additional legal requirements to retain data for longer.

7) Accuracy Data stored on eMobility users should always be accurate and up-to-date. The ISO 15118 standard requires a semi-online charging station to transmit the charging process data at least once a day, so it can be verified that the transaction was valid and the user can be billed accordingly.

8) Security It is important that all data is securely stored and transmitted. Any key material, billing information and location data has to be protected by security measures. Also theft and modification has to be prevented. The security requirements have been addressed in Section 3.4.1.

9) Openness Every user of the eMobility system should be able to access all the information stored about her. For example, a procedure should be in place to request this data. This is one of the EU data protection requirements.

10) Compliance It should be possible to verify that the eMobility system complies with the above requirements. Most of the requirements are legally binding when processing personally identifiable information. The other points may be agreed to by contract or policies.

4.1.2 Summary of eMobility privacy concerns

An introduction to the privacy concerns in eMobility has been given in Section 2.3. Overall the privacy concerns can be summarized as follows:

- While charging PII is transferred to the charging station and the backend.
- Charging occurs frequently, i.e. multiple times a day at different locations. Hence, PII is transferred frequently.
- Charging locations can be recorded to track users and learn their behaviors. The charging station can build user profiles.

Further, the study of the ISO/IEC 15118 standard shows that privacy has not been a design goal and privacy issues exist with the current implementation (see Section 3.4.4). To understand the exact privacy implications a privacy impact assessment is required.

4.2 Privacy impact assessment

Impact assessments have been common in the environmental domain to assess how an action will influence the environment around it [30]. Similarly, technology assessments are done to understand the consequences a new technology will have on society [89]. These strategies has been transferred to privacy to assess how an activity or a technology will impact the privacy of the users [30, 81, 93, 107].

PIA strategies have been developed by several organizations and governments. They often differ in scope, context and goal, depending on the country or organization who developed them or the purpose they were developed for. PIA guides offer direction on how to plan a PIA assessment, when to conduct the assessment and what kind of questions to ask during the process. However, most PIA guides are kept at an abstract and broad level and are aimed at projects and organizational procedures with little focus on specific technologies and technical protocols. Assessments whose main goal is to achieve legal compliance, i.e., fulfilling privacy laws and regulations, form a subcategory of PIAs and are referred to as privacy compliance audits [30, 59]. Overall, a privacy impact assessment should have a broad perspective and considers all privacy issues.

Next to meeting legal requirements, privacy impact assessments are used to identify privacy risks. Privacy risks can lead to loss of reputation and trust, failure of legal requirements and unnecessary privacy invasion [59]. Another purpose of PIAs is to help in the decision process to select the most privacy-preserving design option by examining each option for their privacy risks. An example of this approach is the PIA of a health care system summarized in [36].

If possible a PIA should be integrated into the design of the product[3] to make full use of the assessment by identifying privacy risks at an early stage of the development. Therefore, unnecessary costs for product changes due to privacy concerns can be avoided. Considering privacy during the development of a product follows the privacy-by-design philosophy [58]. The privacy impact assessment is usually conducted by the system owner and the developers [98].

One of the steps to identify the privacy impacts of the product, is to analyze the information needs of the product and relevant stakeholders, and to examine the justifications for the negative privacy impacts. To further analyze the information some PIA guides [99] suggest to answer questions based on the privacy principles discussed in Section 4.1.1. These questions consider, for example, the origin of the data or who can access it. Further PIA steps include finding ways to minimize the collected information and to resolve other privacy risks when possible. Often negative impacts on

[3]Here product is used to refer to whatever activity the PIA is assessing. It could be a technology, e.g., a system, service, or protocol.

privacy are unavoidable. In these cases the aim is to minimize the impact by using privacy-preserving technologies.

The results of the PIA are documented and in some cases published or submitted for approval by a privacy advocate, for example. The results can be used to find less privacy-invasive alternatives, and to design and solve the identified privacy risks.

4.2.1 PIA approach for eMobility

Based on the PIA literature discussed above we now propose a privacy assessment strategy for the eMobility system. The PIA assessment will focus on the ISO/IEC 15118 standard and the architecture discussed in Section 3.2. The assessment has the following structure:

1. *Scope and purpose definition*
   The scope of the PIA assessment describes which part of the system shall be considered, e.g., which protocol or usecase. The assessment may be limited to the study of the user's privacy risks. The purpose explains what the results of the PIA are to be used for, so that the process can be tailored to that need. Any assumptions made for the PIA should be clarified.

2. *Stakeholders*
   Next it is necessary to define the stakeholders relevant to the privacy impact assessment. The stakeholders are those actors that collect, receive, use or share information about themselves or other actors. To simplify the analysis, stakeholders may be grouped when possible.

3. *Information assets*
   Since the privacy impact assessment considers information, these assets need to be identified. Afterwards, it has to be determined which of these assets are PII. The purpose, origin and use of these assets should be examined.

4. *Information requirements and use*
   Next each stakeholder should be considered and their need for information. Here it may be possible to identify points where the amount of available information is greater than the information requirement and possible strategies to lessen the privacy impact can be suggested.

5. *Information handling and other considerations*
   PIAs also consider the legal privacy regulations, such as the way information is handled (storage, retention, safeguards, etc.). These points and any remaining issues are discussed here to complete the assessment.

6. *Evaluation*
   The final step is to summarize and evaluate the privacy risks and to suggest solution strategies. If privacy-invasion is unavoidable the least invasive strategy should be chosen.

4.3 PIA of ISO/IEC 15118

In this section the PIA of the ISO/IEC 15118 eMobility system is conducted. The assessment used the approach proposed in Section 4.2.1.

4.3.1 Scope and purpose definition

This privacy impact assessment analyzes the privacy risks of the eMobility system. The complete eMobility system forms a vast distributed infrastructure with several stakeholders, systems, protocols and national approaches.

For this thesis we are most interested in sensitive information exchanged and collected about the user of the eMobility system, i.e., the driver or owner of the electric vehicle. The privacy analysis focuses on potential privacy invasions from the point of view of the user.

To represent the eMobility system the ISO/IEC 15118 charging protocol [60, 61] and the architecture described in Section 3.2 is used. The PIA concentrates on the specific usecase of charging with automated billing via the eMobility infrastructure (i.e. contract-based payment).

This assessment is done without contact with the developers of the eMobility system or the charging protocol. Hence, it is limited to the study of the available documents and public information. In case the available information is unclear it may be necessary to make assumptions to complete the PIA. Assumptions may be necessary when the ISO/IEC 15118 protocol is too vague, e.g., about the backend, leaves options open or is unclear about details, e.g., certificates relations and validity. We will choose the most realistic and privacy-risky assumption. Any assumptions will be kept as minimal as possible.

The purpose of the assessment is to systematically identify the privacy risks of the ISO/IEC 15118 standard. Further, we hope to identify areas of the protocol where less privacy-invasive approaches can be used and would like to suggest alternatives if possible.

4.3.2 Stakeholders

The stakeholders have been addressed in Section 2.2.1. For this assessment we will concentrate on the main stakeholders involved in the charging architecture as described in Section 3.2. In the following, each stakeholder is introduced and his role with respect to the ISO/IEC 15118 protocol is explained. Further, we will state any assumptions made about the stakeholder in case the available information is unclear.

Electric vehicle user This is the legal entity using the vehicle, i.e., the EV owner and in most cases also the driver of the vehicle. It is also possible that the EV owner is not the driver of the vehicle, for example, for company or rented vehicles. In some cases it may be desired that the owner does not know where the vehicle has charged, because it reveals where the driver has been. But a fleet operator may be interested to know where the driver takes the vehicles to better plan the operation of the fleet. Then, the privacy concerns of the driver are of a lower priority. While these cases have interesting additional privacy properties, for the PIA we focus on the case that the EV user is the driver and owner of the vehicle.

The EV user signed a mobility contract with the mobility operator. According to ISO/IEC 15118, the contract is tied to the user's vehicle. The user makes use of the ISO/IEC 15118 charging protocol indirectly via her electric vehicle. To initiate the charging protocol the user has to plug the vehicle's charging cable into the charging station. Other than this action, no further interaction is required by the charging protocol in the here discussed "plug-and-charge" usecase. The electric vehicle executes the ISO/IEC 15118 charging protocol. The charging parameter negotiation and payment is automatically handled via the protocol. The mobility operator will pay for the charging expenses and bill the user according to the terms defined in the mobility contract. The vehicle can charge at any charging station, no matter if the vehicle is roaming or not. We assume for this assessment that the vehicle is roaming, since this case involves the most stakeholders and information exchange and hence is assumed the most privacy risky. Also, roaming is assumed to be a common scenario.

This privacy analysis considers the privacy invasion of the EV user. However, the EV user in only indirectly involved in the charging protocol. For the PIA we will examine what (sensitive) information is exchanged about the EV. Anything that identifies the EV also identifies the EV user.

Charging station (CS) The charging station is the EV's communication partner in terms of the ISO/IEC 15118 protocol. The CS uses the protocol to communicate with the vehicle to negotiate the charging parameters and to handle the payment. The CS may also contact contact the backend, e.g., its energy provider to negotiate tariff information (outside the scope of this assessment) or the mobility operator to verify the charging contract and to pass on the charging bill. Only the communication with the vehicle is explicitly covered in the ISO/IEC 15118 standard.

CS's energy provider (EP) The ISO/IEC 15118 protocol states that the charging station contacts the power grid to negotiate tariffs and the charging parameters that will be suitable for both the power grid and the vehicle. The standard describes multiple actors, such as the demand clearing house (DCH) used for negotiating the electricity demand, the meter operator who manages the smart meter in the charging station, and the energy provider who delivers the electricity to the charging station. For simplicity, we represent these parties by the energy provider that operates the charging station. The energy provider is likely to be also the operator of the CS's smart meter and has access to the power grid or operates part of it. Hence, the energy provider is capable of negotiating energy parameters on behalf of the power grid.

Further, we assume that the EP receives the payment for the energy use rather than the CS itself. For accountability, we assume that the EP wants to link the energy consumption to a payment, hence the EP makes note of the date and the charging station that obtained electricity. The EP may also want to collect additional information about its customers. For this assessment, we assume that the EP has access to the data recorded by the charging station unless it is protected by security measures, e.g., encryption, or the standard explicitly states that the data remains only accessible to the charging station. For example, the ISO/IEC 15118 standard specifies that signed meter readings are to be deleted if the charging expenses are paid for directly at the charging station.

EV's mobility operator (MO) The mobility operator has a charging contract with the EV user. The ISO/IEC 15118 standard states that the mobility operator may be the same energy provider as the one operating the charging station, a different one or a third party. For this assessment we assume that the mobility operator is different from the CS's EP, so that we consider the maximum of stakeholders and information exchange for the analysis. Further, we assume that the mobility operator is the user's domestic energy supplier. We expect the privacy risks to be the greatest in this case. For example, if the MO is a small local energy supplier, revealing the identity of the MO may reveal the area the user lives in.

Clearing house (CH) The ISO/IEC 15118 standard also mentions several forms of a clearing house that supports the communication exchange between the charging station and actors of the backend, and communication within the backend. For example, the clearing house may be contacted for validating a charging contract. To do so the clearing house must have obtained the information from the mobility operator or may contact the mobility operator. Also, the standard explains that a clearing house may be used as an intermediate to forward the charging bill to the mobility operator. In this scenario the CH forwards a service detail record (SDR) to the mobility operator which contains all the necessary information for paying the energy provider and charging the EV user [60]. The CH will create the SDR from the signed meter readings it receives from the charging station or it directly obtains the SDR from the charging station. The ISO/IEC 15118 standard does not explain this scenario in more detail.

4.3.3 Information assets

To determine the information assets the usecase descriptions [60] and messages of the ISO/IEC 15118 protocol [61] are examined to find out what information exists in the system, where it comes from and with whom it is shared. The protocol describes several usecases ranging from vehicle authentication to charging schedule negotiation and charging specific actions. For this analysis we are most interested in the identification, authentication, authorization and payment communication, as these are likely to contain vehicle identifying information.

Information assets can come in different forms, such as identifiers, certificates, meter readings, timestamps and signatures. Privacy risks are caused by information that will uniquely identify the EV (and hence it's user) and information that indirectly reveals information about the vehicle. The problematic information assets are described in Table 4.1. Empty cells indicate that no information is given in the standard. In some cases assumptions are made. These are printed in italics.

Asset name	Origin	Use(s)	Lifetime	Issue(s)
Provisioning certificate, Cert ID [61] (Bootstrap Cert. in [60])	Installed by OEM in production process.	Used to link vehicle to mobility contract when concluding a mobility contract. Not used for charging communication.	*Lifetime of the vehicle.*	Unique for each vehicle.
Contract ID (as defined in [35, 50]) and contract certificate	Obtained from MO or CH (maybe be updated via CS). May be part of an attribute cert. (cf. [55, 97]).	Ties vehicle to charging contract. EV sends it to CS for (contract-based charging) authentication. CS sends it to the backend (MO/CH) for validity check. (Note: elsewhere the standard says the ID is associated with the electricity consumer and may be vehicle- or customer-specific.)	4 weeks - 2 years	Unique for each vehicle-contract. Reveals the origin country and mobility operator of the contract.
Attribute certificate (Public certificate as defined in [55, 97])	*Obtained from MO, CH or an Attribute Authority.* Can be bound to identify certificate. Link to identity certificate is required to prove ownership of the attribute certificate.	Guarantees that EV is equipped with a pre-established contract, which enables the authorization for power charging even in CS offline scenarios.	Minimal lifetime (e.g., a week to a month).	Unique, contains Contract ID.
Identity certificate	*Obtained from a CA.*	Used at transport layer for mutual authentication of EV and CS. OCSP is used for validating the certificate.		Uniquely identifies the EV. *Not sent to third parties except as part of OCSP.*
Customer ID		Used for identification. Can be ID, certificate or PIN.	*Lifetime of contract*	CS may learn customer identity.
EVCC ID	*Installed during manufacturing of EVCC component.*	The EV's identifier. Contains the MAC address of the EVCC, used during session setup with the CS.	*Lifetime of the vehicle*	The MAC is unique.
E-Mobility operator ID *same as Provider ID*		Unique identification of MO. Identifies the issuer of Contract ID. May be used for roaming. Is sent to CS with Contract ID for EV (contract) authentication.	*Lifetime of MO*	Reveals MO of the EV to parties who receive the ID (e.g., CS and CH).
EVSE ID (as defined in [35, 50]) and Power outlet ID	EVSE operator will fix the power outlet ID.	Unique identification of the charging spot. Power outlet ID is sent to backend during EV authentication process.		Identifies the charging location. EVSE ID reveals the CS's country and EP. Links EV to CS when identifiers are sent together.
EVSE operator ID or Spot Operator ID (this is the EP's ID)		Sent with Power Outlet ID, EV's Contract ID and Provider ID to secondary actors for online EV authentication.		Identifies the charging location of the vehicle. Links EV to CS when identifiers are sent together.

Table 4.1: Identified problematic information assets. (table continues)

Asset name	Origin	Use(s)	Lifetime	Issue(s)
Signed meter readings	EV signs the meter reading of the CS.	Used as proof that the EV consumed the said amount of energy. CS sends it to the EP.		*Reveals the EV to the EP and likely to also reveal the CS to the EP.*
Service detail record	Either generated by CS at the end of the (charging) session or by a CH.	Sent to MO and possibly EV. Contains enough information (details unspecified), so that MO can pay EP and charge EV.		*If involved, CH learns charging details. Reveals EP to MO. May reveal the CS to MO.*
Timestamps	Added by CS to specific ISO/IEC 15118 messages.	Used during SessionSetupRes, for MeterInfoType and PaymentDetailsRes messages.		*Can reveal exact time of charging to the backend when included with transmitted data.*

Table 4.1: Identified problematic information assets. Assumptions are printed in italics. (continued)

Figure 4.1 illustrates how the certificates and identifiers are linked with each other.

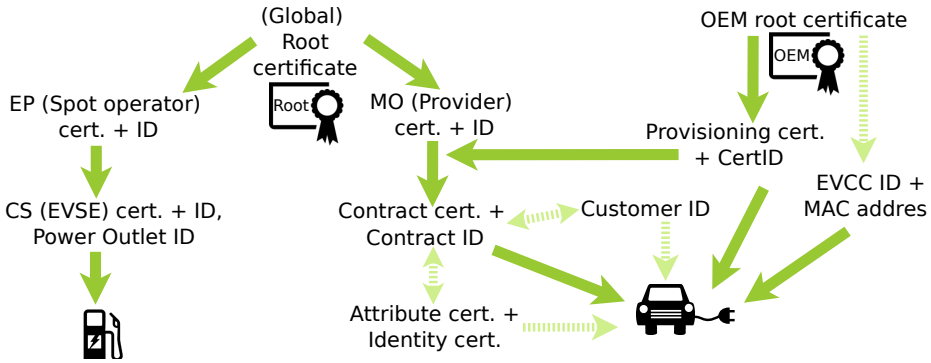

Figure 4.1: The links between the certificates and identifiers. The lighter dashed arrows indicate links which are only vaguely indicated in the ISO/IEC 15118 standard.

After analyzing the information assets described in Table 4.1, it can be concluded that the certificates and identifiers listed below are personally identifiable information. These information assets directly and uniquely identify the electric vehicle and hence the EV user.

- Contract ID and contract certificate
- Identity certificate
- Attribute certificate (linked to the Identity certificate)
- Customer ID
- EVCC ID and MAC address
- Signed meter readings
- Service detail records

The following information assets may reveal privacy sensitive information when linked with a personally identifiable information asset:

- E-Mobility operator ID (Provider)
- EVSE ID and Power outlet ID
- EVSE operator ID (Spot operator)
- Timestamps

For example, if the EVSE ID is linked to a Contract ID during some charging session, the receiver of this information knows that the EV has been charged at the charging station with the EVSE ID. Together with a timestamp the receiver of the information will know exactly when the EV user has been at that location. However, based on the given ISO/IEC 15118 documents timestamps are not included.

Finally, the Provisioning certificate and Cert ID are not used during the charging process. However, they may be sent to the charging station to install or update the Contract certificate and ID. The Provisioning certificate and Cert ID uniquely identify the electric vehicle.

4.3.4 Information requirements and use

Next, the ISO/IEC 15118 protocol's steps are examined in more detail and the minimum information requirements and the actual information amount are compared. This will help to identify parts in the protocol that can be made less privacy-invasive. The analysis will focus on the communication for the (i) mobility contract establishment, (ii) EV authentication and (iii) charging payment including dispute resolution. These parts of the protocol are selected since the assets discussed above are used in these scenarios.

(i) Mobility contract establishment

During the EV contract establishment the vehicle transmits its Provisioning Certificate and the Cert ID (called Bootstrap Certificate in part 1 of ISO/IEC 15118) to its new mobility operator. The mobility operator then creates a Contract Certificate and Contract ID and sends it to the vehicle. This scenario is illustrated in Figure 4.2. The information needs are summarized in Table 4.2.

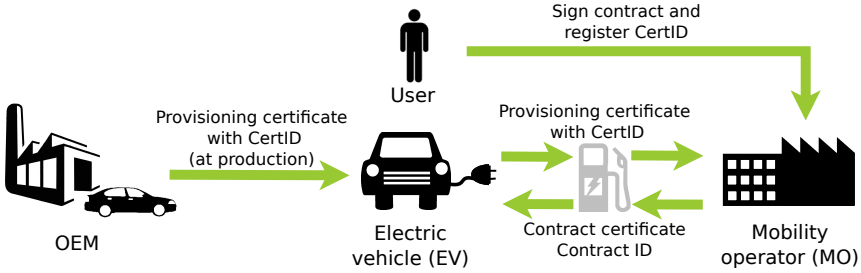

Figure 4.2: The information exchanged during mobility contract establishment.

Scenario	Actual intent	ISO 15118	Minimum required
Creating the contract.	Creating the contract.	– (legal issue)	– (legal issue) Provisioning Certificate needs to be registered with MO (offline).
Link EV to contract, to show charging contract capability.	Give the EV method to prove that it will pay for the charging expenses.	Provisioning certificate to obtain contract certificate and ID.	Contract does not need to be linked to a vehicle identifier. The vehicle only needs a proof that it has a valid contract.

Table 4.2: Mobility contract establishment – Information requirements of ISO/IEC 15118 compared to the minimum needs.

This scenario only happens when a new mobility contract is signed or a contract is extended. This ISO/IEC 15118 standard refers to these steps as "certificate installation" and "certificate update". This is not part of the plug-and-charge usecase. However, during these steps information that uniquely identifies the EV is passed to the charging station. The ISO/IEC 15118 standard states

that other forms of certificate installation/update that do not involve the charging station could be used, but such methods are outside the scope of the standard and are not described any further.

A charging contract does not need to be linked to the EV; the EV only needs to be able to prove that it will pay for the charging expenses. A valid charging contract or certificate can be used to prove this to the charging station. The mobility operator will have to pay for the expenses. This is a legal issues and should be stated in the contract.

Since in most cases this contract establishment is only needed when a new contract is formed and the standard contract duration is two years certificate installations and updates could also be performed offline.

(ii) EV (contract) authentication

To show that the EV has a charging contract it sends its Contract Certificate, Contract ID and the Mobility Operator ID to the charging station. If the charging station is online, it then verifies the validity of the contract by contacting the mobility operator or a clearing house. The charging station also sends its own identifiers to the verifier. This information exchange is depicted in Figure 4.3. When the charging station is offline, it can validate the certificate using the global root certificate. However, the standard does not explicitly state this. Instead the standard describes that the charging station may still transmit the same information as in the online case at a later point in time. Therefore, the only difference between online and offline CS scenarios is that in the online case the validation, and hence the transmission of the information, is real-time. The information requirements are summarized in Table 4.3.

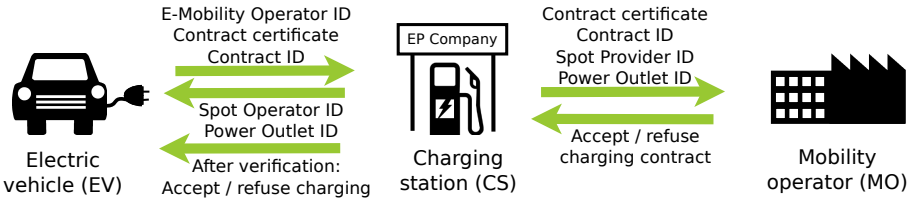

Figure 4.3: The information exchanged for EV (charging contract) authentication according to ISO/IEC 15118.

In addition, for most EV requests the vehicle has to be identified and authenticated. For this the ISO/IEC 15118 standard suggests to use the Contract ID, since it uniquely identifies the EV. This is a privacy risk.

(iii) Charging payment including dispute resolution

The payment process is not clearly explained in the ISO/IEC 15118 protocol. Only part 1 of the standard gives hints about the procedure. The charging station will send the signed meter readings to the energy provider, proving that the EV has consumed energy at the charging station. After the charging session, the charging station will create a service detail record and sent it to the mobility operator. This SDR may also be created by an intermediate clearing house. The standard states that the SDR will contain all the necessary information to pay the energy provider and to bill and inform the EV user about the expenses. However, the exact details about the content of the SDR is not given.

The SDR will at least contain the following information:

- Amount of electricity received
- Chosen tariff (if applicable)
- Amount payable
- Recipient of the payment (the EP)
- Session/transaction number
- Contract/customer identifier

Scenario	Actual intent	ISO 15118	Minimum required
EV shows it has a charging contract.	CS knows EV has a valid charging contract.	Contract certificate, contract ID and MO ID have are sent to CS.	A proof that the EV has a valid contract is enough. Not necessary to include MO identifier (can be derived from Contract ID/Certificate).
Online CS/real-time validation: CS validates the contract details.	CS is convinced contract is valid.	Contract ID, MO ID, CS operator ID and power outlet ID are all send to backend, i.e., the MO.	Not necessary to include CS identifiers when contacting backend. Validation can be done offline (certificate chain).
Offline/semi-online CS: CS validates the contract details.	CS is convinced contract is valid.	Information may still be sent to backend when CS is online, or user interaction is required (e.g., entering a PIN).	Not necessary to include CS identifiers when contacting backend. Validation can be done offline (certificate chain).

Table 4.3: EV contract authentication – Information requirements of ISO/IEC 15118 compared to the minimum needs.

Possibly also the following information is included:

- Charging station's identifiers (Spot Operator ID, Power Outlet ID and EVSE ID)
- Mobility operator's ID
- Date, time and charging duration.
- Any charging specific information (maximum current, etc.)

Figure 4.4 illustrates the charging payment communication exchange. The information requirements are summarized in Table 4.4.

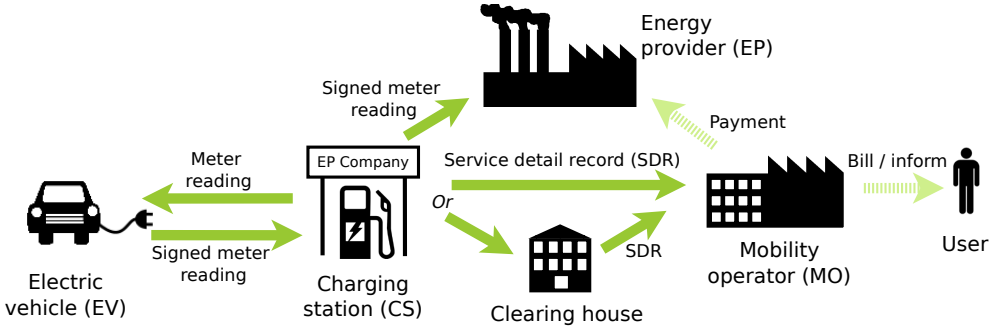

Figure 4.4: Charging payment – The information exchanged for the charging commitment and payment according to ISO/IEC 15118.

Sending the signed meter readings to the EP is an accountability measure. Now the energy provider knows that it can expect a payment for the charging session. The energy provider will already know about the energy being consumed, because it is able to communicate with the charging station via the smart meter. If the payment does not occur the energy provider can use the singed meter readings to prove that the EV has consumed the energy and request the payment. On the other hand, this procedure is privacy-invading for the EV user.

Scenario	Actual intent	ISO 15118	Minimum required
Send the signed meter readings to the EP.	Show the EP which EV has consumed energy. Give EP a means to prove the energy consumption in case of dispute.	Meter readings signed by EV are sent by the CS to the EP.	CS can send otherwise authenticated meter readings.
Send the SDR to the MO (possibly via CH).	Tell the MO about the charging expenses for paying EP and informing/billing EV user.	Meter readings signed by EV are sent by the CS to the MO.	Bill or signed meter readings. Not necessary to use CS to forward the bill.
Payment of the EP by MO.	MO has to pay the EP.	SDR contains enough information. Details unspecified.	MO has to know who to pay, how much to pay and which EV user to charge.

Table 4.4: Charging payment – Information requirements of ISO/IEC 15118 compared to the minimum needs.

4.3.5 Information handling and other considerations

Overall, the ISO/IEC 15118 standard gives little information about how information is handled, i.e., how, where and what information is store and what safeguards are used to protect it. However, the privacy requirements established in Section 4.1.1 call for adequate measures. For example, the "Openess" requirement (see Sect. 4.1.1 requirement 9) suggests that the user may know and see all data recored about her and her EV. This may be difficult to realize with the distributed eMobility infrastructure.

Further, the use of private information requires consent from the user (requirement 2). This is not directly addressed by the ISO/IEC 15118 standard. However, the standard explains the possibility of external identification means (EIM), for example, using an RFID card, NFC, SMS or via entering a PIN. Since these EIMs require user interaction, a human-media-interface could be used to ask for the user's consent, when using the EIM. However, little to no user interaction is one of the requirements for electric vehicle charging systems (cf. Section 3.1).

The requirement "Limited retention" (requirement 5) specifies that data should only be kept for as long as it is required. The ISO/IEC 15118 standard fulfills this for direct payment scenarios. If the EV user pays the charging expenses directly at the charging station, e.g., with a debit or credit card, the standard specifies that the signed meter readings will be deleted and not forwarded to the backend [61]. For contract-based payment it is unclear at what point the charging station and the energy provider, who received a copy, delete the signed meter readings.

Another potential issue is the use of the Contract ID. The Contract ID is used for contract-based charging but also for EV identification and authentication. However, considering the "Purpose specification" requirement (1), the standard states the purpose correctly. The Contract ID is to be used "*to enable charging and related services (incl. billing)*" [60].

It is difficult to say how the ISO/IEC 15118 standard handles the other privacy requirements based on the given information.

4.3.6 Evaluation

Though the ISO/IEC 15118 standard states that "*Private information and user data shall only be readable by the intended addressees*" and "*Private information shall be transferred only when necessary*" [60], the privacy impact assessment has shown that privacy risks exist and the information

use can be limited.

In step 3 of the PIA (see 4.3.3), the potentially privacy-invasive information assets were examined. The ISO/IEC 15118 standard explains that the Contract ID may be linked either to a vehicle or a customer. However, overall the standard uses the definition that a charging contract is tied to the EV. Both scenarios will uniquely identify the EV user. The analysis has shown that the Contract ID is used at multiple points of the protocol: for EV charging authentication and contract validation. The ISO/IEC 15118 standard describes that the Contract ID is used as a means for general EV identification/authentication purposes. For example, when the EV sends a "Service discovery" request it also performs the identification procedures and sends its Contract ID to the charging station [61]. When providing the contract information also the Mobility Operators ID (Provider ID) is communicated to the charging station. The charging station can also deduce who the MO is by considering the Contract ID format [50] or looking at the Contract Certificate's issuer field (assuming that the MO is the issuer of the certificate). In case the MO is a small local energy supplier, this may reveal in which city or area the EV user lives. Overall, the use of the Contract ID is very privacy-invasive.

Further identifiers exist that uniquely identify the EV, such as the EVCC ID, the Provisioning Certificate and Cert ID, the Identity Certificate and the Customer ID. The Provisioning Certificate including the Cert ID and the EVCC ID are given to the EV during production by the OEM and most likely remain the same during the lifespan of the vehicle. The Provisioning Certificate is only used for mobility contract establishment. However, the ISO/IEC 15118 protocol offers certificate installation options via the eMobility infrastructure using the ISO/IEC 15118 protocol. The EVCC ID also uniquely identifies the vehicle and contains the MAC address of the vehicle. If the Contract ID is renewed after the maximum lifetime of 2 years expired, the MAC address and the Provisioning Certificate will still be the same and could be used to link the vehicle's old and new Contract ID.

The ISO/IEC 15118 standard is unclear about how and when the Attribute and Identity Certificates are used. Similarly, the use of the Customer ID is not explained. The standard only states that the Customer ID is to be used for identification purposes. We assume that the Customer ID is unique for each EV user. The use of will be privacy-invasive.

During contract validation the charging station includes its own identifiers (Spot Operator and Power Outlet ID) when communicating with the backend. Every receiver of these messages will be able to link the EV and the CS. Since an online charging station will send these messages in real-time, i.e., while the EV is connected to the charging station, the exact location and time can be documented for the vehicle. Any stakeholder that records this can track the vehicle. The mobility operator (and possibly the clearing house) is one of the receivers of this data. For the mobility operator it may be interesting to know where his clients are charging to adjust the tariffs, for example.

Finally, when the vehicle is charging it keeps signing the meter readings of the charging station. The singed readings are sent to the energy provider by the charging station. This means that the energy provider learns the EV's identity. The energy provider is also likely to know which charging station sent the meter readings. The signed meter readings are used for dispute resolution. If the bill is not paid the energy provider can use the signed meter readings as proof that the EV has consumed energy. The energy provider can find out the identity of the EV and request the payment. This dispute resolution mechanism is not required when the bill is paid directly at the charging station. Then, the signed meter readings are deleted and not sent to the energy provider. Further, the charging station sends a service detail record to the mobility operator, either directly or via a clearing house. If the charging station directly contacts the mobility operator, the MO will learn the charging location, e.g., based on the CS's IP address or using included CS identifiers. The service detail records will contain enough information for the MO to pay the charging bill and to inform its customer about the charging session. The details of these records are not specified in the ISO/IEC 15118 standard. It can be assumed that at least the EV, the energy provider and the electricity amount is mentioned in the record.

The identified privacy invasions can be summarized by the following privacy invasion types (PIT):

PIT 1) *Direct identification of the EV:*

Every stakeholder receiving an EV-identifier can uniquely identify the EV. If multiple recordings are stored, the vehicle can be tracked.

PIT 2) *Revealing the CS (charging location) in conjunction with an EV-identifier:*
Similar to the case above, but also the charging location is known, allowing more privacy-invasive tracking. For example, if the CS is revealed to the MO, this informs the MO where the EV has been.

PIT 3) *Revealing the MO in conjunction with an EV-identifier:*
This may reveal where the EV owner lives (see above for assumptions about the MO).

PIT 4) *Revealing the EP in conjunction with an EV-identifier:*
This may reveal the charging location if the EP is a small local energy provider.

The privacy impact analysis has shown that in particular the charging contract validation is privacy-invasive, as it informs the mobility operator about the charging location and possibly also the exact time. It is not necessary to inform the mobility operator about the charging station. Further, the payment communication, including the dispute resolution mechanism, shows signs of equally privacy-invasive approaches. The energy provider will learn the EV's identity and the mobility operator will know the energy provider. In the case the energy provider and mobility operator are small local energy companies, this will reveal private information about where the EV user has been and where the user lives.

In order to lessen the privacy impact of the ISO/IEC 15118 charging protocol, the information exchange should be limited to the minimum required for operation. Any identifiers or certificates that are not needed to fulfill the goals of the protocol can be eliminated. The forth PIA step "Information requirements" (see 4.3.4) has documented this. In addition, any privacy-invasive messages should be replaced with privacy-preserving alternatives.

As a next step, we will propose and analyze several privacy-preserving alternatives for the identified privacy-concerns.

4.4 Possible privacy-preserving alternatives

The ISO/IEC 15118 charging protocol needs to be modified in order to be privacy-preserving. However, before starting the design of our privacy-preserving charging protocol, we shall consider the parts of the ISO/IEC 15118 protocol that cause privacy concerns and examine privacy-preserving alternative mechanisms that fulfill the same purpose. For each alternative the advantages, disadvantages and the privacy-preserving properties are examined. In our privacy-preserving protocol we can make use of the most suitable privacy-preserving alternatives.

Examples found in scientific publications, commercial proposals for eMobility solutions [60, 103, 106, 108], and solutions proposed for privacy concerns in other areas, such as electronic tolling [76, 96], have been used to develop these privacy-preserving alternatives. In addition, privacy enhancing technologies, such as e-cash [27, 28, 66], have been examined.

The PIA identified the following steps of the ISO/IEC 15118 protocol to be privacy-critical:

- EV contract authentication
- Billing communication
- Dispute resolution

The ISO/IEC 15118 standard uses a "no secrets" approach. The vehicle reveals its contract credentials during EV contract authentication. For billing, the charging station has direct contact with the mobility operator to submit the charging bill. Then, the mobility operator pays the energy provider. Hence, all parties know about each other. For dispute resolution, the energy provider can uncover the vehicle's identity from the signature on the signed meter readings to contact the mobility

operator or the vehicle owner. The ISO/IEC 15118 charging scenario is illustrated in Fig 4.5.

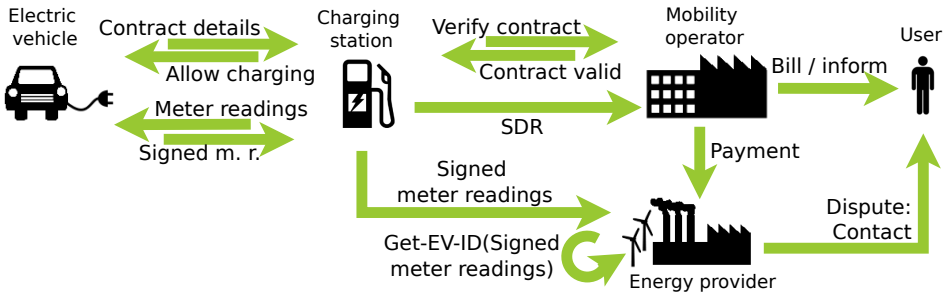

Figure 4.5: The ISO/IEC 15118 charging scenario.

Next, we will discuss privacy-preserving alternatives for each of the privacy-critical ISO/IEC 15118 protocol steps.

4.4.1 EV contract authentication

The concern with contract authentication is that the electric vehicle has to show its credentials to the charging station. These credentials uniquely link to the vehicle and can be used to track the vehicle. Instead of showing the actual contract credentials, the following privacy-preserving alternatives can be used.

(i) Direct payment

When using a charging contract the vehicle has to show the contract credentials to the charging station. The charging station then may verify the credentials with the backend. To avoid this need for contract authentication, the charging expenses could be paid directly at the charging station. Then, also no backend communication is required. Since direct payment is also a potential solution for the billing communication concerns, the advantages and disadvantages are discussed in the following section.

(ii) Token

Instead of showing the actual contract credentials the vehicle obtains a charging token from its mobility operator. The token is a form of a one-time pass that allows the vehicle to charge without revealing the Contract ID. The tokens could also be distributed by a certificate authority.

First, the vehicle obtains one or more tokens from the mobility operator. Then, when charging the vehicle passes a token to the charging station. The charging station can preferably verify the token locally or by contacting a responsible authority in the backend. When the token is valid the charging is allowed and the contract authentication phase is completed. This approach is illustrated in Fig. 4.6.

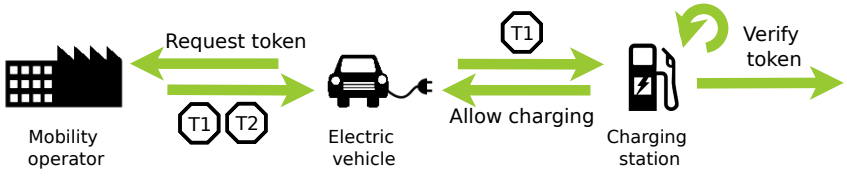

Figure 4.6: Using a token for contract authentication.

A token offers anonymity for charging contract authentication. The charging station does not learn who the electric vehicle or the electric vehicle's mobility operator is. However, there always needs to be a sufficient amount of tokens in the vehicle and every charging station requires a means to verify the token. If only one token is given out for each token request, the vehicle has to request a token before every charging session. This requires a communication link with the mobility operator each time. The connection could be established directly from within the vehicle via the cellular network or via the charging station's Internet connection. The latter approach may cause privacy concerns, if the mobility operator can deduce the charging station's location from the token request communication. Further, after the charging session the mobility operator still needs to receive the charging bill.

(iii) Proof

Similar to the token approach, the vehicle could show a proof that it has a charging contract, e.g., a certificate signed by a global authority that certifies that the vehicle has a valid charging contract without disclosing the Contract ID. This proof could be installed in the vehicle as part of the contract establishment or be requested by the vehicle, e.g. via the cellular network or the charging station's Internet connection.

During contract authentication, the electric vehicle gives the proof to the charging station and is allowed to charge if the proof is valid. Again, the charging station checks the proof locally or contacts a responsible authority in the backend. If the verification is successful the vehicle is allowed to charge. This approach is depicted in Fig. 4.7.

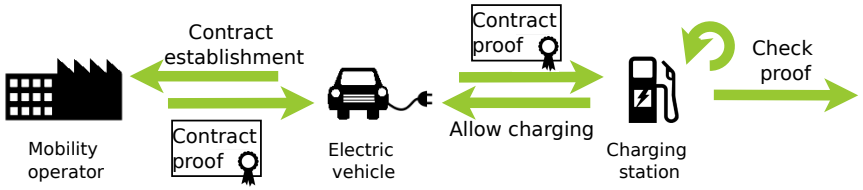

Figure 4.7: Using a proof for contract authentication.

Using a proof offers a privacy-preserving alternative for contract authentication. No contract credentials are disclosed to the charging station. To validate the proof, the charging station needs access to the root certificates. The ISO/IEC 15118 standard also requires root certificates access. However, when using a signed certificate as proof, the certificate cannot be created by the mobility operator, so that the charging station does not learn the mobility operator's identity. Further, if a contract is terminated early, the proof has to be revoked. The ISO/IEC 15118 protocol already requires charging station to use CRL or OCSP to check the status of certificates (see Sect. 3.4.3). The same approach can be used for revoked proofs.

(iv) Involve a trusted third party

If the vehicle does not trust the charging station with its contract credentials, a trusted third party can be involved. The electric vehicle then shows its credentials to the trusted party who then informs the charging station that the contract is valid. This contact authentication approach is shown in Fig. 4.8.

A trusted third party offers privacy towards the charging station, however the contract details have to be disclosed to the third party. All stakeholders have to trust the third party. Further, the charging station always requires a real-time connection to the third party. Hence, if the trusted third party is unavailable the charging expenses cannot be paid via the mobility operator. Also, the trusted third party needs to be able to verify the credentials and might have to contact the mobility operator for verification of the contract. In this case, the mobility operator may be able to correlate

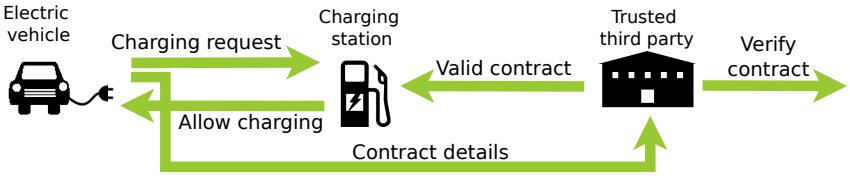

Figure 4.8: Using a trusted third for contract authentication.

the verification request with the charging bill based on the date and time. Further, the trusted third party may become a bottleneck and is a potential single point of failure (SPOF) of the charging system.

4.4.2 Billing communication

There are two privacy concerns with the billing communication. First, the charging station sends the SDR to the mobility operator, which means both parties know about each other. Second, the mobility operator learns who the energy provider is, because the energy provider is the payment receiver. The second concern is more difficult to solve, because the monetary flow of information will always link the paying and receiving parties.

(i) Direct payment

Direct payment could make use of cash, debit or credit card or a prepaid card. The user can, for example, use cash payment similar to payments at conventional gas stations. For the prepaid approach, the user has a prepaid account for paying the charging expenses. The information could be stored on an RFID card that the charging station can read.

As discussed in the previous section, direct payment at the charging station eliminates the need for contract authentication. In addition, it eliminates the need to forward the bill to the mobility operator and the subsequent payment to the energy provider. Hence, this approach requires no communication with the backend and the charging station may be semi-offline. The direct payment approach using a prepaid card is illustrated in Fig. 4.9.

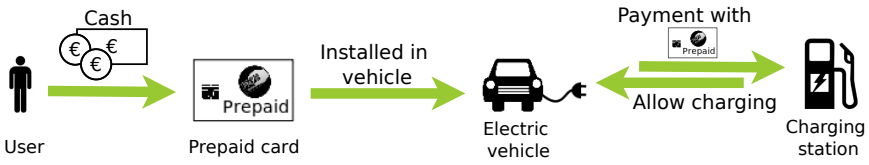

Figure 4.9: Direct payment with prepaid.

The direct payment approach protects the user's privacy, if a privacy-preserving payment method is used, i.e., when using a debit or credit card, the payment is not privacy-preserving; the transaction can be linked to the EV user. Using a prepaid account is privacy-preserving, since it is not necessary to link the prepaid account to an individual. To be completely privacy-preserving, the user should top-up the prepaid balance with untraceable payment methods, such as cash. The prepaid account can be made accessible to the vehicle to automate the payment. Prepaid as payment method for EV charging has been suggested by [60, 86, 103, 106].

A drawback of direct payment is that in most cases it requires direct user interaction to pay the charging expenses. One of the eMobility requirements is to limit the need for user interaction. Another disadvantage of prepaid payment is that the user needs to make sure that there are sufficient funds on the prepaid account.

(ii) E-cash

Instead of using one of the above mentioned payment methods, e-cash can be used for anonymous electronic payments, either directly at the charging station or otherwise by the mobility operator to pay the energy provider.

E-cash (electronic cash) is a privacy-preserving approach used for anonymous electronic payments. The NetCash system [66] and Chaum's blind-signature based system [27, 28] are two electronic cash implementations. The goal of e-cash is to replicate the characteristics of cash transactions for electronic payments. The privacy of the user should be protected, so that the identity of the payee, Alice, does not have to be revealed and no transaction can be linked to another. At the same time the system needs to be secured against double spending and other forms of cheating. First, Alice goes to a bank and exchanges physical cash for NetCash, for example. This procedure is similar to exchanging money for a different currency. The bank operates an online currency server that creates the electronic cash and signs it, similar how bank notes are marked and numbered. Now, Alice can spend the NetCash. The receiver of the money, Bob, can check whether the money has been spent by contacting a currency server during the transaction. If the payment is valid, Alice will obtain the paid service and a receipt of the purchase. Bob can directly use the NetCash for other payments.

Chaum's e-cash system also has semi-offline double spending protection and reveals the identity of the cheater when e-cash coins have been used before. When Alice goes to the bank to obtain e-cash, she has to embed her identity in the coin. The identity cannot be seen from the coin. However, if Alice tries to spend the same coin twice with Bob, her identity will be revealed to Bob with high probability. In Chaum's system, Bob has to contact the bank to exchange the coin for a new coin with his identity embedded, before his is able to spend the money.

In the eMobility system, the vehicle can be given access to the user's e-cash wallet to directly pay the charging station. This approach has the same advantages as direct payment with prepaid. However, this approach also requires the vehicle to have sufficient electronic cash funds to cover the bills, or the vehicle has to obtain electronic cash before intending to pay a bill.

Instead of using e-cash for direct payment at the charging station, it can also be used by the mobility operator to pay the energy provider. Then, the energy provider does not learn who the mobility operator is. However, the mobility operator still has to receive the bill and has to know who to pay.

The two e-cash cases are illustrated in Fig. 4.10.

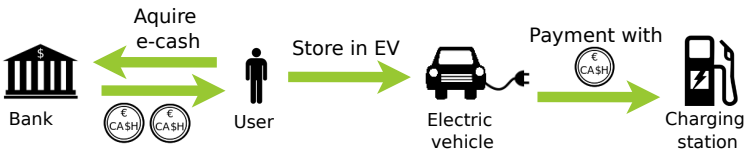

Figure 4.10: Using e-cash for payment.

Further, electronic cash payment requires an e-cash infrastructure to be in place for exchanging and verifying the electronic cash. E-cash has been suggested as a means of payment in [74, 108].

(iii) EV submits the bills

When using a mobility contract, the mobility operator has to receive the charging bill, so that the mobility operator can pay the energy provider. In the ISO/IEC 15118 protocol the charging station sends the bill in form of a SDR to the mobility operator. In order to eliminate this information flow between the charging station and the mobility operator, the bill should not be send by the charging station. Instead at the end of the charging process the vehicle obtains the bill from the charging station and submits it to its mobility operator. The charging station's energy provider gets paid by the mobility operator and the user is billed according to the charging contract. This approach is based on the electronic tolling approach described in [76]. It is depicted in Fig. 4.11.

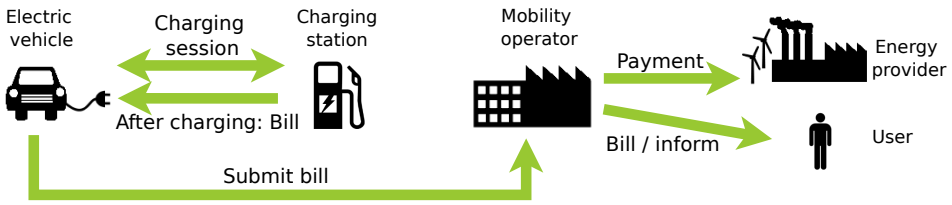

Figure 4.11: The EV submits the bill to the mobility operator.

This approach for submitting the bill is privacy-preserving, because only the charging station and the mobility operator do not learn about each other. However, the electric vehicle can cheat by not handing in the bills. If the charging station does not know the identity of the mobility operator or the electric vehicle it cannot follow up on outstanding payments. An additional dispute resolution mechanism is required to present the electric vehicle from cheating.

(iv) Involve trusted third party

Similar to the approach for EV contract authentication, a trusted third party can be used for forward the bill to the mobility operator. The charging station sends the bill to the trusted third party and the vehicle informs the trusted third party which mobility operator it uses. The trusted third party then sends the bill to the rightful mobility operator.

As discussed above, using a third party offers privacy towards the charging station and when using it for the billing communication both the charging station and the mobility operator do not learn about each other. However, the same disadvantages as for using a third party for EV contract authentication apply here (see Sect. 4.4.1).

(v) Involve payment intermediary

In order to eliminate the information leaked by the payment of the mobility operator to the energy provider, a payment intermediate can be used. Then the payment receiver is hidden from the mobility operator and the mobility operator sends the payment together with the hidden receiver to a payment handler. This payment intermediary then uncovers the payment receiver and completes the payment. This approach is shown in Fig. 4.12.

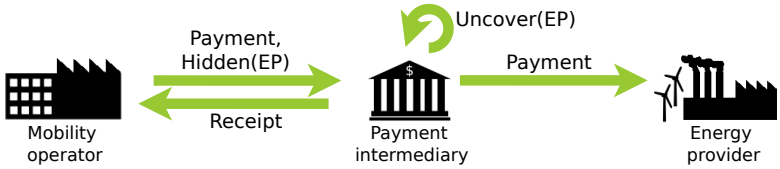

Figure 4.12: Using a payment intermediary.

This approach eliminates the privacy concerns relating to the monetary flow of information. However, adding a payment intermediary means the eMobility infrastructure is changed. Further, similar to a trusted third party, all stakeholders have to trust the payment intermediary to not keep the money for himself and the payment intermediary may also be a potential single point of failure.

(vi) Energy supplier aggregation

Another approach is to aggregate smaller local energy suppliers to create a larger association. Other than offering privacy benefits, joining an association can be economically beneficially for a small energy provider, because the association can collaborate to set up and maintain the charging infrastructure.

Instead of revealing the mobility operator, the electric vehicle informs the charging station which association its mobility operator belongs to and sends the mobility operator identifier in hidden form, e.g., encrypted. The charging station sends the bill to the association including the hidden mobility operator identifier and its hidden energy provider identifier. The association uncovers the mobility operator identifier and the bill is forwarded to the mobility operator. The mobility operator then sends the payment to the association the energy provider belongs to. The energy provider association uncovers the energy provider identifier and the payment is transfered to the rightful energy provider. This billing approach is illustrated in Fig. 4.13.

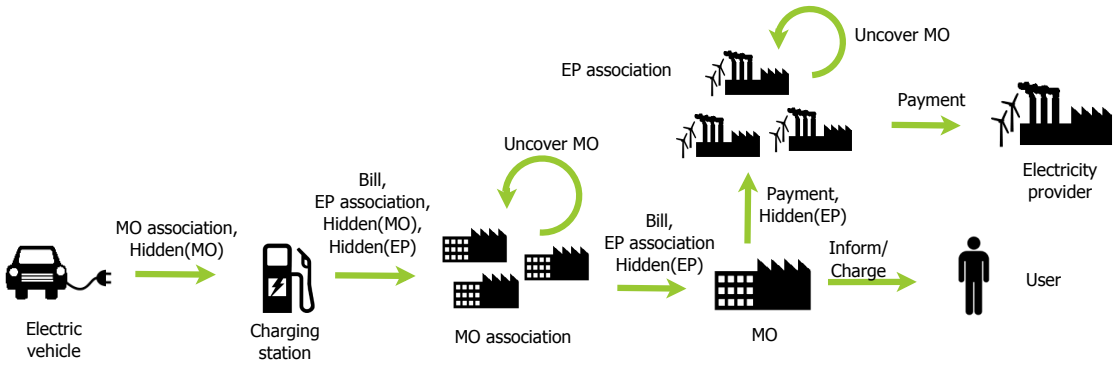

Figure 4.13: Using aggregation of energy suppliers to hide exact energy provider and mobility operator.

Revealing the exact energy provider or mobility operator leaks information about the vehicle's charging location or domestic energy supplier (i.e., the mobility operator). Aggregation hides the individual energy provider or mobility operator within a larger group of energy providers. The bigger the group, the more privacy is offered. The group size directly affects the amount of privacy this approach can offer. If a small energy supplier decides not to join an association, there is no privacy for its customers. Similarly, when regional associations are formed or the energy provider and mobility operator belong to the same association the amount of privacy offered can be reduced. Also, the communication links may still reveal information about the charging station.

Aggregation on its own may not offer the desired level of privacy, but it can be applied as an additional privacy-protection measure.

4.4.3 Dispute resolution

The ISO/IEC 15118 protocol's dispute resolution mechanisms raises privacy concerns, because the energy provider learn the electric vehicle's identity from the signed meter readings. During the charging session the charging station repeatedly asks the vehicle to sign the meter readings. At the end of the charging session the signed meter readings are sent to the energy provider. To be privacy-preserving the charging station and the energy provider should not learn the identity of the electric vehicle.

(i) Direct payment

The ISO/IEC 15118 protocol already specifies, that the charging station does not forward the signed meter readings if the charging expenses are directly paid at the charging station, but the charging station still learns the vehicle's identity. In general, if the payment is fulfilled at the charging station, no dispute resolution mechanism is required. However, the electric vehicle may have insufficient funds. To protect against this, small micro payment should be done during the charging session, before continuing the power delivery.

(ii) Involve trusted third party

Similar to the trusted third party cases described above, also for dispute resolution a trusted third party can be involved. For example, the signed meter readings can be send to a third party instead of to the charging station and the energy provider. The third party informs the charging station that the signatures are valid and the energy provider only receives the meter readings from the charging station without signature. However, the same disadvantages as described earlier apply when using a third party for dispute resolution.

(iii) EV commits

In order to avoid disclosing the EV's identity by signing the meter readings the vehicle makes a commitment to the meter readings. This method is used by the electronic tolling approach described in [76] or for electronic vehicle insurances in [96]. The charging station can check the commit but it does not see the identity of the vehicle. At the end of the charging the commits are send to the energy provider. In case of dispute a dispute resolver is contacted to reveal the identity of the vehicle. Then the energy provider or the dispute resolver contacts the EV user to settle the dispute. This approach is depicted in Fig. 4.14.

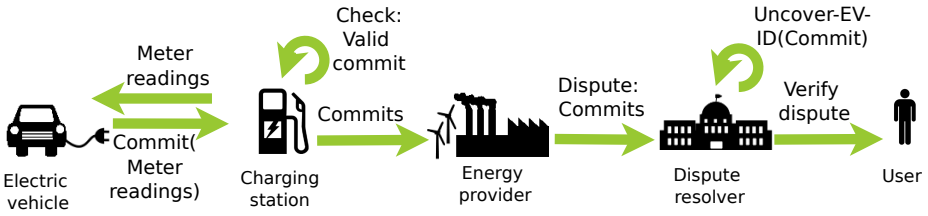

Figure 4.14: Using EV commitments for dispute resolution.

Using anonymous commitments offers privacy. Only if there is a dispute the vehicle's identity is revealed. Since the dispute resolver is only involved in cases of disputes, it is unlikely that it becomes a bottleneck of the system and there are no real-time requirements for the operation of the dispute resolution. However, the eMobility infrastructure needs to be changed to include the dispute resolver and all stakeholders have to trust the dispute resolver. Further, the dispute resolution has to be secure so that a malicious energy provider cannot abuse the feature, by requesting the EV identity for every commit.

4.4.4 Summary of the alternatives

Several privacy-preserving alternatives for the ISO/IEC 15118 protocol steps have been discussed. Table 4.5 summarizes the alternatives.

Case	Protected information				Advantages	Disadv. & Requirements
	EV	MO	CS	EP		
EV contract authentication						
ISO	✗	✗	✗	–		Semi-online CS
i Direct payment	✓	–	–	–	*see Billing Communication case i*	
ii Token	✓	✓	–	–	No contract details revealed	New token for each charging session; local verification or online connection to verifier
iii Proof	✓	✓	–	–	No contract details revealed	Revocation mechanism; local verification or online connection to verifier

Table 4.5: Summary of privacy-preserving alternatives (table continues)

iv Trusted third party	✓CS ✗TTP	✓CS ✗TTP	✓MO ✗TTP	–	No contract details revealed to CS	TTP can be bottleneck/ SPOF; additional infrastructure (TTP); online connection to TTP
Billing communication						
ISO	✗	✗	✗	✗		Semi-online CS
i Direct payment	✓	–	–	–	Offline CS possible	No billing via contract; sufficient funds (prepaid); some user interaction
ii e-cash used by EV	✓	–	–	–	Offline CS possible	No billing via contract; sufficient funds (e-cash); e-cash infrastructure; some user interaction
ii e-cash used by MO	–	✓	–	✗	EP does not learn payee identity	e-cash infrastructure; some user interaction
iii EV submits bill	–	✓	✓	–	CS and MO do not communicate	EV can cheat; occasional EV (Internet) connection to MO
iv TTP	–	✓CS ✗TTP	✓MO ✗TTP	–	*same as EV contract authentication case iv*	
v Paym. interm.	–	✓EP ✗PH	–	✓MO ✗PH	Monetary information flow is hidden	PH can be bottleneck/ SPOF; additional infrastructure (PH)
vi MO/ EP agg.	–	(✓)	–	(✓)	Not exact MO/EP revealed	Large aggregation size
Dispute resolution						
ISO	✗	✗	–	–		No secrets
i Direct payment	–	–	–	–	No dispute resolution needed	Insufficient funds protection
ii TTP	✓CS/EP ✗TTP	–	✗TTP	–	*same as EV contract authentication case iv*	
iii Dispu. resolver	✓CS/EP ✗DR	✓CS/EP ✗DR	–	–	DR only used for disputes	Additional infrastructure (DR)

Table 4.5: Summary of the privacy-preserving alternatives

While all alternatives have disadvantages, the combination of two or more of the alternatives may eliminate some of the disadvantages. Similarly, the requirements may be shared by one of more alternative so that additional efforts are decreased. For example, a suitable dispute resolution mechanism can protect against the EV cheating in the Billing Communication case iii.

4.5 Summary

This chapter has conducted a privacy impact assessment of the ISO/IEC 15118 charging protocol. The analysis has shown that several privacy concerns exist and not all privacy requirements are fulfilled by the ISO/IEC 15118 standard. The protocol can be improved to be less privacy invasive by following the PII minimization suggestions of the PIA. However, the PIA also shows that the ISO/IEC 15118 protocol steps contract authentication, billing communication and dispute resolution remain privacy-invasive after minimizing the amount of exchanged information. Therefore, several more privacy-preserving approaches for the identified protocol steps have been examined.

To address the identified weaknesses, the next chapter will propose step-wise enhancements and alterations to the original ISO/IEC 15118 charging scheme following the suggestions of the PIA and the most suitable privacy-preserving alternatives discussed above.

CHAPTER 5

Privacy-preserving charging protocol

In this chapter our privacy-preserving charging protocol is discussed. The PIA analysis conducted in the previous chapter concluded that the ISO/IEC 15118 protocol is privacy-invasive and gave suggestions on how to make the electric vehicle charging communication more privacy-preserving. The goal is not to develop a new charging protocol, but to reuse the ISO/IEC 15118 standard as much as possible. To address the identified weaknesses, we propose step-wise alterations and enhancements to the original ISO/IEC 15118 charging scheme following the suggestions of the PIA and using the most suitable privacy-preserving alternatives examined in the previous chapter (see Section 4.4). The step-by-step modifications are discussed in Section 5.1.

To complete the design of our privacy-preserving charging protocol – the POPCORN protocol, several concrete security and privacy technologies are examined, e.g., anonymous credentials. This is discussed in Section 5.2. Finally, the POPCORN protocol is summarized in Section 5.3. Here, the POPCORN protocol and the ISO/IEC 15118 protocol are compared.

5.1 ISO/IEC 15118 protocol modifications

This section discusses the step-by-step modifications and enhancements of the ISO/IEC 15118 protocol. As a first step we minimize the amount of privacy-invasive information being exchanged in the ISO/IEC 15118 protocol. Next, the privacy-invasive information is replaced with privacy-preserving alternatives without changing the protocol behavior. Then the privacy-risky information flow is modified to preserve the user's privacy. Finally, the payment related information leak is examined and suggestions are made to eliminate it.

5.1.1 Modification 1: Minimization of PII exchange

The PIA analysis has shown that the ISO/IEC 15118 protocol transmits more information than necessary for several of the protocol steps (see Section 4.3.4). The first modification of the ISO/IEC 15118 protocol is to remove all non-essential personally identifiable information assets without changing or breaking any of the ISO/IEC 15118 protocol behavior. In this section, we discuss these modifications in detail. As for the PIA, we focus on the communication for (i) mobility contract establishment, (ii) EV charging authentication and (iii) payment of charging expenses.

(i) Mobility contract establishment During the ISO/IEC 15118 mobility contract establishment the Provisioning Certificate (or Bootstrap Certificate [60]) and the Cert ID are given to the mobility operator. The mobility operator (or a certificate authority on behalf of the MO) then generates the Contract Certificate and ID. The contract is tied to the electric vehicle. This means that the charging contract uniquely identifies the electric vehicle.

The ISO/IEC 15118 standard allows the electric vehicle to install and update the Contract Certificate via the charging station. Either the charging station receives the contract credentials on behalf of the electric vehicle and forwards them to the vehicle, or the vehicle itself sets up a connection to

the respective mobility operator or certificate authority to obtain the Contract Certificate and ID. The standard also suggests that other means, external to the ISO/IEC 15118 protocol, can be used to install the contract credentials in the electric vehicle.

As first modification, it shall be mandatory that the electric vehicle itself contacts the mobility operator (or the certificate authority) and not the charging station on behalf of the electric vehicle. This avoids disclosing the Provisioning Certificate to the charging station (PIT 1, see Section 4.3.6). The ISO/IEC 15118 standard describes as part of the trust and architecture assumptions, that the electric vehicle can transfer data without the charging station having access to it. However, the mobility operator may be able to trace what charging station the electric vehicle has used to request the contract credentials. Another option is to not use the charging station's Internet access, but to use another Internet connection, e.g., the EV user's home Internet or the user's cellphone.

The modified contract establishment is illustrated in Fig 5.1.

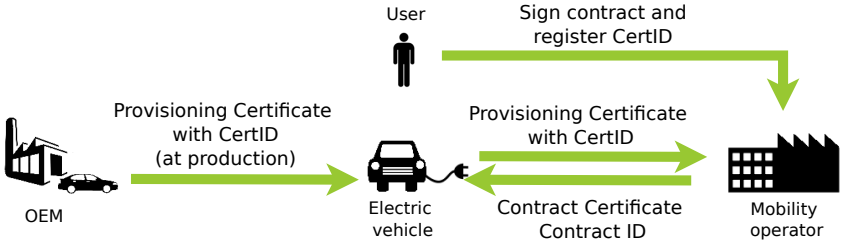

Figure 5.1: The information exchanged for contract establishment after modification 1 (cf. Fig. 4.2).

(ii) EV contract authentication The PIA has shown that online contract authentication is privacy-invasive, because the mobility operator learns the EV's identifiers together with the charging station and energy provider identifier (PIT 2 and 4, see Section 4.3.6). However, using offline validation the charging station may still validate the contract at a later point in time with the backend. Therefore, offline validation is equally privacy-invasive. Figure 4.3 shows the information transmitted according to the ISO/IEC 15118 protocol.

We propose the following modifications to the contract authentication procedure. During contract validation with the backend the charging station shall not include its own identifiers. The mobility operator or clearing house that verifies the contract does not need to be informed about the Spot Operator ID or the Power Outlet ID. In addition, the electric vehicle shall not send the E-Mobility Operator ID to the charging station. Since the charging station receives the Contract Certificate and ID, it will be able to deduce the mobility operator from the certificate issuer field or from the Contract ID format [50]. Finally, the charging station shall verify the Contract Certificate locally, therefore eliminating contact with the backend for this procedure altogether. The charging station can perform local certificate verification based on the certificate chain. The ISO/IEC 15118 standard states that the charging station has access to the global root certificates. In order to check if a Contract Certificate has been revoked, the charging station can use the Online Certificate Status Protocol (OCSP) or a Certificate Revocation List (CRL), as already specified in the ISO/IEC 15118 standard [61]. Another option is to reduce the lifetime of the Contract Certificate to a short period of time, therefore avoiding the need for certificate revocation means.

The modified EV contract authentication procedure is shown in Fig 5.2.

(iii) Payment of charging expenses According to the ISO/IEC 15118 protocol the charging station has all the information to generate a bill, i.e., in the form of a service detail record (SDR), and sends it to the mobility operator. The content of the SDRs is not specified in the standard. Possible values of the SDR have been discussed in Section 4.3.4. Further, the energy provider is informed about the charging session and receives the signed meter readings. The electric vehicle's signature reveals the

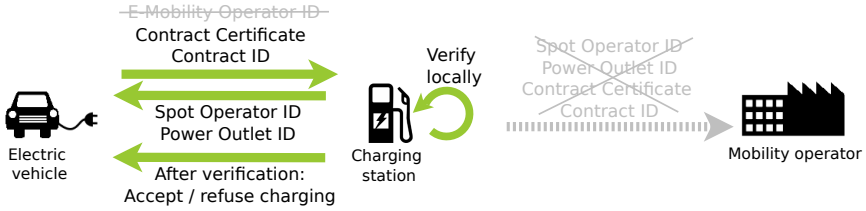

Figure 5.2: The information exchanged for EV (charging contract) authentication after modification 1. The gray messages indicate the parts that have been removed (cf. Fig. 4.3).

vehicle's identity (PIT 1, see Section 4.3.6). Figure 4.4 shows the information transmitted according to the ISO/IEC 15118 protocol.

As part of this first modification, the exact content of the SDR has to be specified. Only the minimum of required information shall be contained in the SDR. We propose the following SDR content:

- Amount of electricity received
- Chosen tariff (if applicable)
- Amount payable
- Recipient of the payment (the EP)
- Session/transaction number
- Contract/customer identifier

In addition, the charging station's identifier shall not be included in the SDR. Including it would be a PIT 2. However, the mobility operator may be able to deduce the charging location from the source IP address when receiving the SDR from the charging station.

Evaluation

The first modification has removed some of the privacy-sensitive information from the exchanged messages, therefore limiting the information flow to the necessary minimum as identified in the PIA, without breaking any of the ISO/IEC 15118 protocol features.

Modification 1 can be summarized by taking the following actions:

- Make it mandatory for the electric vehicle to obtain the contract credentials itself, i.e., do not transfer the Provisioning Certificate/ID to the charging station. If possible, use home Internet connection for retrieving contract credentials.
- Do not transfer E-Mobility Operator ID to the charging station.
- Do not include charging station's identifiers when contacting backend for contract authentication.
- Verify contract certificates locally at the charging station.
- Only include specified content in SDR, i.e., do not include charging station information in the SDR.

By avoiding the use of the charging station to obtain the contract credentials the charging station cannot learn the Provisioning Certificate, one of the PII assets. The Provisioning Certificate could be used to track the electric vehicle even after the Contract ID has been changed. The standard already requires the charging station to have access to the global root certificates. Therefore, the vehicle's certificates can be verified locally. Since the ISO/IEC 15118 standard already requires the charging station (and electric vehicle) to be capable of using OCSP and CRL [61], the same approach can be used for Contract Certificate revocation.

Further, the SDRs have been specified and no charging station identifier has been included. However, there is still a communication exchange between the charging station and the mobility

operator. Both may learn each other's identity together with the electric vehicle's identifier resulting in a PIT 2 and 3. The applied modifications could not eliminate these privacy-invasions.

In addition, there is still PII being transferred. For example, the Contract ID and the signed meter readings both uniquely identify the electric vehicle. Therefore, only limiting the information exchange to the minimum does not remove the privacy concerns. More fundamental changes to the ISO/IEC 15118 protocol are necessary to avoid using PII in the protocol messages. Another modification step is required.

5.1.2 Modification 2: Privacy-preserving alternatives for PII use

As the evaluation of Modification 1 has shown, there is still uniquely-identifying information being used (i.e. PIT 1). Where possible messages containing such PII have to be replaced with privacy-preserving alternatives, such as those discussed in Section 4.4. As part of the second modification we examine the protocol messages for PII that can be replaced without changing the functions of the protocol.

The PIA has identified the personally identifiable information assets of the ISO/IEC 15118 standard (see Section 4.3.3). The PII includes the Contract Certificate/ID, the EVCC ID and MAC address, the signed meter readings, as well as, the SDR. In addition, the PIA identified the Attribute Certificate including the Identity Certificate and the Customer ID. However, no specific ISO/IEC 15118 protocol messages could be found that contain the Attribute Certificate, the Identity Certificate or the Customer ID. Also, the SDR cannot be simply replaced without other changes to the eMobility architecture, because the mobility operator will always need to know whom to pay and which of his customer he has to charge for the expenses. Therefore, this modification focuses on (i) the Contract Certificate and ID, (ii) EVCC ID and MAC address and (iii) the signed meter readings.

(i) Contract Certificate and ID The Contract Certificate and ID uniquely identify the electric vehicle. These credentials are used during EV identification and authentication for charging. In order to find a privacy-preserving alternative the actual intent of the contract credentials should be examined. By presenting the vehicle's contract credentials, the charging station can verify that the vehicle has a valid charging contract. A valid charging contract implies that there is some entity, i.e., the mobility operator, that has the legal obligation to pay for the charging expenses. This is specified in the mobility contract. However, it is not necessary that the exact contract credentials are used, as long as the same intention can be achieved. Instead of presenting the actual credentials, the vehicle could obtain a token or a form of proof, as examined in Section 4.4.1 case ii and iii, which confirms that the vehicle has a valid charging contract. The mobility operator or a certificate authority on behalf of the mobility operator could issue such a proof. The electric vehicle then presents the proof to the charging station and the charging station verifies the proof locally.

The privacy-preserving contract establishment and contract authentication is depicted in Figure 5.3.

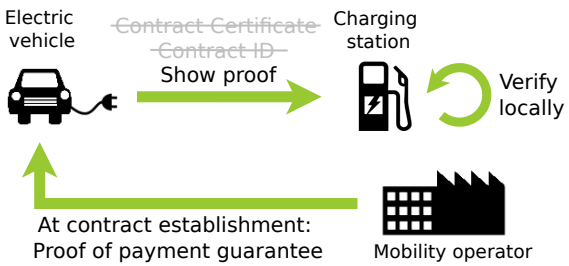

Figure 5.3: The information exchanged for EV (charging contract) authentication (incl. contract establishment) after modification 2. The gray messages indicate the parts that have been removed.

Another use of the Contract ID is to identify what charging tariff applies. For example, extra roaming fees may apply or contract conditions that set the maximum current [61]. The electric vehicle will have to inform the charging station about its applicable conditions. The mobility operator is the one to add extra charges when the vehicle is roaming, therefore the mobility operator has to be informed, but not the charging station. Since the SDR is sent to the mobility operator by the charging station, the electric vehicle encrypts the roaming status and sends the encrypted value to the charging station, which includes the value in the SDR. The roaming status is encrypted so that only the mobility operator can read the value and the charging station cannot learn any additional information about the vehicle. Another case requiring tariffs to be taken in to account, is when the mobility operator and the charging station's energy provider have arranged special prices, e.g., an all-day flatrate. In general, the prices in the eMobility system are affected by demand and supply and the charging station may vary the prices accordingly. If the electric vehicle knows it is eligible for a special tariff, it has to prove this to the charging station without revealing its identity in the same way it proves that it has a valid contract during contract authentication. If the vehicle does not know about the applicable tariffs and it has Internet access to its mobility operator, it can contact the mobility operator and request clarification.

(ii) EVCC ID and MAC address The EVCC ID contains the MAC address of the electric vehicle and is used when the electric vehicle is connected to the charging station for session setup. Since the MAC address is statically defined according to the RFC 4291 [61] it uniquely identifies the vehicle [54]. The EVCC ID and the MAC address need to be randomized for each charging session, so that a charging station cannot link any charging sessions to the same vehicle. We will discuss technical approaches to randomize the MAC address in Section 5.2.

(iii) Signed meter readings The signature on signed meter readings reveals the electric vehicle's identity. The signed meter readings are used as part of the ISO/IEC 15118 protocol's dispute resolution mechanism. By signing the meter readings the electric vehicle commits to the electricity consumption. This in turn gives a security to the energy provider that he will be able to link the consumption to a vehicle. If the charging expenses are not paid for the energy provider can obtain the electric vehicle's identity and follow up on the payment. Since the signed meter readings are privacy-invasive, they shall be replaced with a privacy-preserving alternative. The electric vehicle has to commit to the electricity consumption without directly revealing its identity to the energy provider (cf. Section 4.4.3 case iii). Instead the energy provider will have to contact a trusted third party, e.g., a dispute resolver (DR), who has the means to reveal the vehicle's identity. This scenario is illustrated in Figure 5.4.

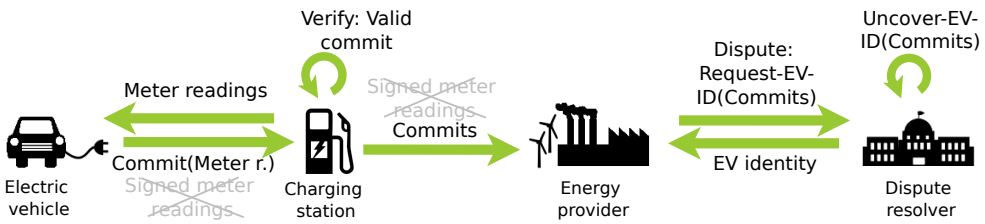

Figure 5.4: The information exchanged for dispute resolution after modification 2. The gray messages indicate the parts that have been removed (cf. Fig. 4.4).

Evaluation

The second modification has removed the remaining personally-identifiable information from the ISO/IEC 15118 protocol. The PII has been replaced with privacy-preserving alternatives.

Modification 2 can be summarized by taking the following actions:

- Do not use the actual Contract Certificate and ID, but use a privacy-preserving proof that the electric vehicle has a valid charging contract.
- The EVCC ID and MAC address shall be randomized for each charging session.
- Do not send the signed meter readings to the energy provider, but another form of commitment that does not reveal the vehicle's identity to the energy provider. A dispute resolver has the means to uncover the identity for the energy provider in case of dispute.

By avoiding the use of the actual contract credentials and by randomizing the EVCC ID and MAC address the charging station cannot link two charging sessions to the same vehicle. Therefore, the charging contract authentication is now privacy-preserving. However, using an anonymous proof makes it more difficult to apply special charging tariffs. If the vehicle is solely responsible to inform the mobility operator about its roaming status, the electric vehicle can cheat to avoid paying extra roaming fees. The possibilities to prevent cheating need to be discussed as part of the technologies analysis in Section 5.2. Considering the other tariff case, the charging station may be able to deduce which mobility operator the electric vehicle uses, because the charging station's energy provider only has one such tariff agreement with a specific mobility operator. The charging station does not learn the vehicle's exact identity, but some privacy is given up for better prices. To reduce the loss of privacy, the eMobility system can agree to fixed tariff classes, so that multiple energy providers and mobility operators use the same tariffs.

The second modification has changed the dispute resolution mechanism, so that the energy provider cannot deduce the vehicle's identity from the signed meter readings. The privacy-invasion of type 1 (direct identification) are eliminated at the cost of adding another party – the dispute resolver. However, the energy provider may abuse the dispute resolution mechanism to obtain the vehicle's identity. The dispute resolver does not verify whether there is an actual dispute. This has to be addressed as part of the next modification.

Further, using the privacy-preserving contract credentials the charging station will not be able to include the Contract ID in the SDR. The charging station also will not know the mobility operator and hence cannot send the SDR there directly. Previously, it was possible to deduce the mobility operator using the Contract ID format or the Contract Certificate's issuer field. Overall, the information flow between the charging station and the mobility operator is privacy-invasive, because both parties learn each other's identity in conjunction with a PII of the vehicle (PIT 2 and 3). The ISO/IEC 15118 standard describes the possibility of using a clearing house to send the SDRs. The electric vehicle's Contract ID and the identity of the mobility operator could be made visible only to the clearing house. The ISO/IEC 15118 protocol's information flow shall be examined for remaining privacy-risks as part of the next modification.

5.1.3 Modification 3: Privacy-preserving information flow

As identified during the previous modification, the information flow may also be privacy-invasive. In the current state of the protocol most privacy concerns have been removed. PII is only being used during dispute resolution and for the payment. The evaluation of the second modification has shown that the energy provider can abuse the dispute resolver to obtain the electric vehicle's identity. This information flow needs to be modified. Also, the SDRs need to be examined to find a privacy-preserving solution for transmitting the billing relevant data to the mobility operator. This modification examines (i) the service detail record transfer and (ii) the dispute resolution.

(i) Service detail records transfer The ISO/IEC 15118 protocol suggests that the charging station or a clearing house generates and transmits the SDR to the mobility operator. The SDR has to contain enough information, so that the mobility operator can pay the energy provider. One possible solution is to hide the contract and mobility operator information from the charging station. The clearing house then uncovers the mobility operator identity, but not the Contract ID, so that the clearing house does not learn the identity of the vehicle. For example, the Contract ID could be encrypted by the electric vehicle with the public key of the mobility operator.

Another solution is to let the vehicle transfer the SDR. Since one of the eMobility system requirements (see Section 3.1) is to limit the need for extra infrastructure, such as the clearing house in the previous case, letting the electric vehicle itself deliver the SDR fulfills this requirement (see Section 4.4.2 case iii). After the charging session the charging station generates the SDR including only the known fields. When delivering the SDR to the mobility operator the electric vehicle appends its Contract ID. The electric vehicle can use the user's home Internet connection to transfer the SDR, since it is not necessary that the SDR is transferred directly after the charging session. In addition, not sending the SDR in real-time also reduces the timestamp information leak, as discussed during the PIA (see Sect. 4.3.3). If the electric vehicle does not submit the bill, i.e. the vehicle cheats, the energy provider will contact the dispute resolver with the vehicle's charging commits to obtain the electric vehicle's identity. The dispute resolver will uncover the vehicle's identity from the commits (see Fig. 5.4).

The privacy-preserving SRD transfer is illustrated in Figure 5.5.

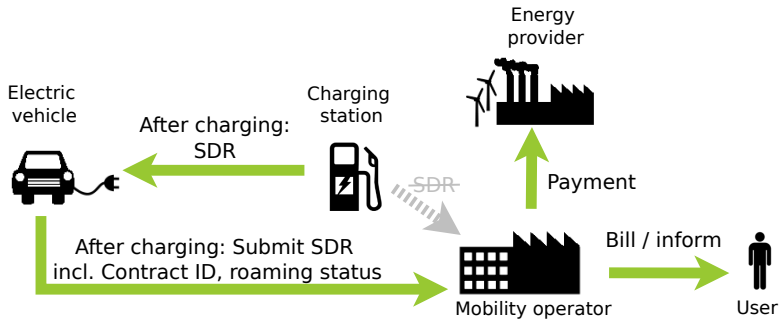

Figure 5.5: Transferring the SDR to the mobility operator after modification 3. The gray messages indicate the parts that have been removed.

(ii) Dispute resolution In the current protocol the energy provider can request the identity of the electric vehicle, even if there is no dispute. To prevent this abuse, the dispute resolver shall not send the identity to the energy provider. Instead the dispute resolver shall uncover part of the electric vehicle's information to find out which mobility operator is obliged to pay the energy provider. The dispute resolver then contacts the mobility operator to verify the dispute. The mobility operator then has to check his records for the payment in question. If the mobility operator did pay he may send a transaction receipt to the dispute resolver, that proves the payment has been made. If the electric vehicle never submitted the bill the mobility operator can fulfill the payment and contact his customer for clarification. For example, the electric vehicle's communication controller may be faulty or tampered with. In case the mobility operator is cheating and never paid the charging expenses the dispute resolver may uncover the complete identity of the electric vehicle and contact the electric vehicle user directly for verification about the payment. Overall, further disputes about payments or breaches of contract are legal issues and are outside the scope of the protocol.

The modified dispute resolution procedure is shown in Figure 5.6.

Evaluation

The third modification has removed the remaining privacy concerns from the ISO/IEC 15118 protocol. The information flow has been changed to be privacy-preserving.

Modification 3 can be summarized by applying the following changes:

- Let the electric vehicle transfer the SDR to the mobility operator, instead of the charging station or a clearing house.

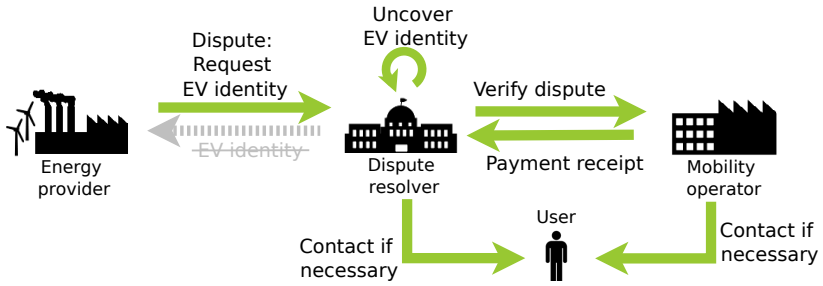

Figure 5.6: The information exchanged for dispute resolution after modification 3. The gray messages indicate the parts that have been removed.

- The dispute resolver shall not send the electric vehicle identity to the energy provider, but instead shall investigate the dispute by contacting the mobility operator or the electric vehicle user if necessary.

Now, the protocol messages are privacy-preserving. Only the dispute resolver will learn the energy provider, the mobility operator and if necessary the identity of the electric vehicle. The dispute resolver is a trusted party and the functions could be handled by a certificate authority. However, the mobility operator will still learn the identity of the energy provider when receiving the SDR (PIT 4). The mobility operator will not know the exact charging location. But if the energy provider is a small local energy provider, the mobility operator can conclude in which region the electric vehicle user has been. Also, the energy provider can see who sent the payment. However, the energy provider is only able to link the payment to a charging session; not to a specific vehicle. Another modification is necessary to also eliminate the information flow stemming from the money transfer.

5.1.4 Modification 4: Extra privacy

The evaluation of modification 3 has shown the payment allows the mobility operator to link the energy provider with the electric vehicle (PIT 4). In order to hide the personally identifiable information leakage due to the cash flow, this section examines (i) a modification using MO/EP aggregation and (ii) the use of a payment intermediate.

(i) Energy provider aggregation In order to hide the exact energy provider, several energy providers can form an association together. Especially for small local energy providers joining an association can have other practical benefits. The association can help with providing the necessary expertise and infrastructure for the eMobility system (see Section 4.4.2 case vi). The SDR contains the name or identifier of the association and a hidden value of the exact energy provider. The hidden value could be encrypted, for example. The mobility operator pays the association and includes the hidden energy provider identifier with the payment information. The association uncovers the identifier and forwards the payment to the actual energy provider. The association is not allowed to inform the energy provider which mobility operator sent the payment.

This scenario is illustrated in Figure 5.7.

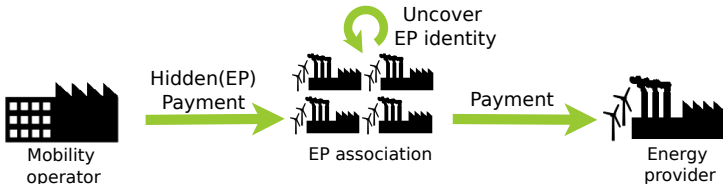

Figure 5.7: Using energy provider associations to hide the actual energy provider.

(ii) Payment intermediary An even more privacy-preserving option is to use a payment intermediary to hide all payment-related information flows. The SDR contains the recipient of the payment in a hidden form. The mobility operator then transfers the payment to the payment intermediary with the hidden energy provider value. The payment intermediary uncovers the name of the energy provider and forwards the payment to the rightful recipient.

This approach is illustrated in Figure 5.8.

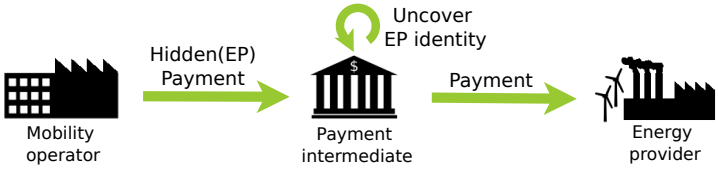

Figure 5.8: Using a payment intermediary to hide the monetary information flow, based on modification 4.

Evaluation

The protocol's last privacy concern is the information leakage related to the payment from the mobility operator to the energy provider. Two options have been suggested.

The first option requires the use of energy provider associations. Using an energy provider association means that multiple energy providers can be aggregated to one, therefore, hiding the actual recipient. However, most mobility operators are energy distributors themselves. The aggregation effect may be lost if the energy provider and the mobility operator are part of the same association, since the mobility operator may be able to uncover the hidden value. Further, the amount of privacy depends on the amount of energy providers joining an association. The more energy providers join an association the more anonymity the association can provide. On the other hand, an energy provider that does not join any association will be exposed directly, offering no payment privacy. Also, regional associations may be created, hence giving away the approximate location where the electric vehicle has been. One possible solution to these disadvantages is to allow an energy provider to join multiple association. A random association is selected for every charging session.

Option (ii) introduces another party to the eMobility system – a payment intermediary – to forward the payment to the rightful recipient. This hides the two parties involved in the payment from each other. The payment intermediate is a trusted party and will know each transaction party, but not the actual electric vehicle and charging station concerned. If all payments have to go through the payment intermediate, it may become a bottleneck for the eMobility system. Multiple payment intermediaries can be used to lessen such availability concerns. A payment intermediate could try to cheat by keeping the money he received from the mobility operator. The energy provider will file a dispute with the dispute resolver. For every payment, the mobility operator expects to obtain a payment receipt from the payment intermediate. If the receipt did not arrive, the mobility operator can report this during dispute resolution and the payment intermediate has to be contacted. If the payment intermediate send a fake payment receipt, the mobility operator is no longer liable for the missing payment. The energy provider has to be asked to check his accounts and the payment intermediate has to be contacted about the payment receipt.

The second option offers the most privacy-preserving solution and together with the rest of the ISO/IEC 15118 modifications ensures complete charging privacy for the eMobility user.

5.2 Technologies

When implementing the proposed privacy-preserving protocol concrete security and privacy technologies have to be used. This section analyzes the protocol steps and examines possible technologies

that fulfill the purpose.

5.2.1 Contract credentials as payment guarantee

The main use of credentials is to prove some attributes about a person to someone else, e.g. a passport proves that the person in question is a citizen of a specific country. One of the problems with credentials is that often more attributes are revealed than is required by the requested service. Alice may show her passport to the bartender to prove she is legally allowed to drink. However, when inspecting the passport the bartender also learns her name, her nationality, her exact birthday and other irrelevant information.

In the digital world, digital certificates are used to proof attributes about an entity, e.g., a web server proves it belongs to your bank. In the eMobility system, the vehicle shows its Contract Certificate to the charging station. The certificate not only shows that the vehicle has a valid charging contract, it also reveals the identity of the vehicle, the identity of the mobility operator, and the expiration of the charging contract. The charging station can uniquely identify the vehicle and link the charging session of the vehicle. For the proposed privacy-preserving charging protocol, the contract proof has to be anonymous and unlinkable, i.e., it must not reveal the identity of the electric vehicle or any other uniquely identifying information to the charging station.

Anonymous credentials [17, 20] have been developed for anonymous authentication and can be unlinkable depending on the implementation [3, 101]. Based on the minimization privacy principle (see Section 4.1.1), anonymous credentials allow selective disclosure of credential attributes, while hiding the other attributes. In addition, anonymous credentials can be used to disclose properties of credential attributes without revealing the actual attribute value.

The use of anonymous credentials is illustrated with an example: Before Alice can use her anonymous credentials, she has to get them certified by the trusted issuer Ivan. Ivan checks that it is really Alice requesting the anonymous credentials and that her attributes are correct. The attributes contain, for example, her name, birthday, address, social security number and her nationality. The issuing procedure is very similar to the one for requesting a digital certificate, except then an anonymous credential is linked to Alice's secret key. At the end, Ivan sends her the anonymous credentials.

Now, Alice would like to buy a wine in Bob's web shop. Using a conventional certificate Alice has to reveal all her information to Bob. However, Bob only needs to know whether she is legally allowed to order wine. Using her anonymous credentials, Alice can only disclose that she is above the legal drinking age. Her exact birthday and any other information remain unknown to Bob. Bob verifies the credential and sees that Ivan certified the credentials. Bob knows that Ivan is a trusted issuer of credentials. Hence, Bob accepts the credentials and the order is prepared to be shipped by the courier Charlie. With the same anonymous credentials Alice informs Charlie about her name and address without revealing any other information. This scenario is depicted in Fig. 5.9.

When Bob asks Alice to show an attribute, she does not send the actual credential with its values to Bob. Instead, Alice creates a zero-knowledge proof-of-knowledge that the disclosed attribute was certified by Ivan and that she knows the secret key it is linked to [20]. Not showing the actual anonymous credentials means that Alice can go to Bob a second time and he will not be able to link the two occasions. Unlinkablity is fulfilled. Alice can also prove some property about her attribute without revealing the attribute's value [17]. For example, using her birthday attribute, she can calculate that her age is equal or above the legal drinking age, as required for the scenario above. The zero-knowledge proof is sent to Bob. Bob can verify the proofs using Ivan's public key.

Since anonymous credentials do not contain unique identifiers, standard CRLs do not work. However, several revocation strategies exist. One possibility is to limit the lifetime of the anonymous credentials [64]. The validity period is included as an attribute in Alice's credentials. During each authentication, Alice proves that her credentials are not expired in addition to her other attribute proofs. Another approach is to let Alice prove to Bob, that her anonymous credentials are not on a CRL [70]. A discussion of revocation mechanisms can be found in [64].

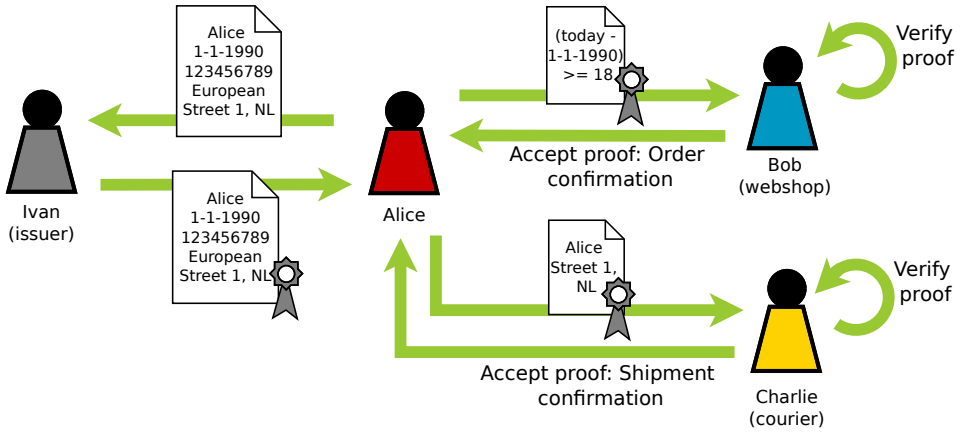

Figure 5.9: Selective disclose of information using anonymous credentials.

In the POPCORN protocol, the vehicle obtains its anonymous credentials during contract establishment. The anonymous credentials certify that the vehicle has a valid charging contract. The credential attributes include the identifier of the mobility operator, the expiration date of the contract, special tariffs and other contract conditions. When the electric vehicle authenticates for contract-based charging, it proves to the charging station that the charging contract is valid (i.e., the expiry date is larger than the current date), but hides the other attributes. To make use of special tariffs, e.g., a flatrate, the vehicle has to prove to the charging station that it is eligible for a special tariff.

Anonymous credentials can also be used to prevent the vehicle from cheating when it adds the roaming status to the SDR. The charging station has to have its own anonymous credentials that contain attributes about the charging station, such as the location (country). One approach is to ask the charging station to prove that it is part of the no-roaming-fee list of charging stations. However, this requires the vehicle to have a list of all no-roaming-fee providers and has to show that list to the charging station. Showing the list can make the vehicle distinguishable from other vehicles. Another approach is to ask the charging station to create a (non-interactive) proof about some attributes that will convince the mobility operator that the vehicle is or is not roaming, without revealing too much information about the charging station and to the charging station. For example, if the vehicle does not have to pay roaming fees for Dutch charging stations, it can ask the charging station to prove that it is a Dutch charging station. If the charging station is located in the Netherlands it will be able to create such a proof. The electric vehicle appends the proof to the SDR and the mobility operator can verify the proof when receiving the SDR.

Two credential revocation strategies have been described above. The revocation list approach has the disadvantage that the charging station need to keep the list updated and an additional message exchange between the vehicle and the charging station is required to pass the list to the vehicle. For the POPCORN system, the anonymous credentials lifetime shall be limited to a short period of time. Since the vehicle occasionally requires an Internet connection to send the SDRs, the vehicle can also use this connection to receive updates for its anonymous credentials. Non-interactive updates can be used, so that the vehicle only needs to download the update information and the update can be installed while offline [64]. A validity period attribute has to be included as an additional attribute in the anonymous credentials. During authentication the vehicle proves in addition to the expiration date proof also that the validity period has not passed.

Creating attribute proofs and verifying them requires more computations than conventional certificates. However, optimizations and implementations suitable for low-resource environments, e.g., smart cards, are being developed [4, 8], so that anonymous credentials can be used for digital passports or ID-cards [17]. Since the vehicle is likely to use similar proofs during contract authentication, it may be possible to compute some parts in advance or while the vehicle is still performing other low computation tasks, e.g., a power line safety check. Overall, creating a proof and verifying it should not take longer than a few seconds [3, 4]. The time it takes also depends on the implementation

used and the amount of attributes included in the anonymous credential.

Two implementations of anonymous credentials exist: U-Prove [67] and Idemix [22, 57]. Idemix (Identity mixer) offers multi-show unlinkability and attribute property proofs. U-Prove makes use of blind signatures instead of zero-knowledge proofs and currently does not offer these functionalities [3]. The Idemix anonymous credentials system has been described above. The implementation has been developed as part of the PRIME and PrimeLife research projects [77]. The ABC4Trust Project is continuing the development of attribute-based credentials [1].

The POPCORN protocol makes use of the Idemix anonymous credentials system. Using anonymous credentials instead of conventional certificates, allows the vehicle to selectively disclose attributes about its charging contract, while the identity of the vehicle remains hidden. The anonymous credentials system is provably secure under the strong RSA assumption [20].

5.2.2 Proof of energy consumption

The main use of a signature is to show that the signer attests to the content of the signed document, e.g., when signing a contract. Signatures can also be used to certify the origin of the signed message. For example, when Alice signs her mobile phone contract she gives her consent to the contractual terms. When Bob sends Charlie a birthday greeting card, Charlie knows that the card comes from Bob based on the signature.

In the digital world, electronic signatures are used to attest authentication (i.e. origin) and non-repudiation of the signed message. The ISO/IEC 15118 protocol requests the electric vehicle to sign the meter readings of the charging station during the charging loop. After the charging session they are sent to the energy provider. The signed meter readings prove that the vehicle confirms that it received the specified amount of electricity, and hence has to pay for the consumption. The energy provider can directly learn the identity of the electric vehicle from the signature. For the proposed privacy-preserving protocol, the identity of the signer shall be hidden from the energy provider or charging station, but the signature still has to be verifiable by all parties. Further, the signatures must be unforgeable and unlinkable. The electric vehicle must not be able to sign claiming to be someone else and the charging station must not be able to link to charging sessions to the same vehicle. Another important characteristic is that the signature can be attributed to a specific vehicle in case of dispute by a trusted third party, i.e., the dispute resolver.

Group signatures [5, 9, 18, 21, 29] have been developed to allow any member of a group to anonymously sign on behalf of the group. For example, in a group with the participants Alice, Bob and Charlie. Alice can sign on behalf of the group and is anonymous among the members of the group. The bigger the group, the better the anonymity. To an outsider, Oscar, or a group member the signatures of the different group members look the same, i.e., unlinkability is fulfilled. Further, Oscar can verify that the signatures are genuine. However, Oscar cannot create valid group signatures, i.e., unforgeability is given. A group manager, Greg, is responsible of adding or removing members to the group and is able to reveal the identity of the original signer in case of disputes.

First, Greg chooses the security parameters and the group's secret and public key. The group's public key is accessible by anybody, including the outsider Oscar, and it is used to verify a group signature. Next, Alice generates her group private key in cooperation with Greg and obtains a membership certificate. Only Greg is able to identify Alice from her signatures. Bob and Charlie follow the same steps as Alice to join the group. Now, each member can sign for the group. When Bob creates a group signature, he performs a non-interactive zero-knowledge proof-of-knowledge of his member certificate and his group private key [23, 40]. The same applies to the other group members. If Charlie cheats, Greg can reveal Charlie's identity using the group's secret and public key. Depending on the implementation used, it is possible to revoke a group member's signing ability [9]. Otherwise, new group keys have to be generated and the genuine members have to join the group again [40]. Another important property of group signatures is exculpability, i.e., Alice nor Greg can sign on behalf of Bob. Further, it is not possible to create a group signature that Greg cannot link to one of the group members. A general group signature scenario is shown in Fig. 5.10.

In the POPCORN protocol, group signatures replace the conventional signature on the meter

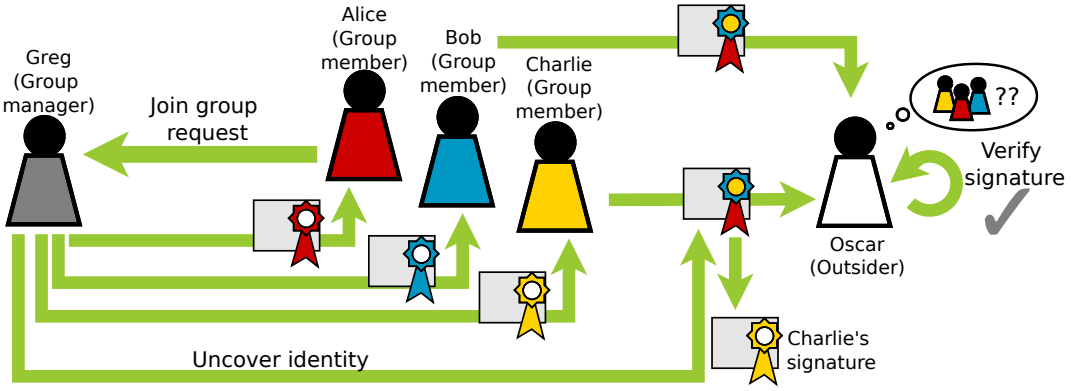

Figure 5.10: Anonymous signing with group signatures.

readings. When the vehicle obtains its contract credentials it also joins the group of all electric vehicles and obtains its membership certificate. During the charging loop the charging station asks the vehicle to sign the meter readings. The vehicles performs a group signature, which the charging station can verify with the group's public key. At the end of the charging session, the charging station sends the group-signed meter readings to the energy provider. The energy provider can also verify the signatures if necessary. If the charging expenses are not paid, the energy provider contacts the group manager, i.e, the dispute resolver. The dispute resolver is able to reveal the vehicle's identity and can verify the dispute by contacting the vehicle's mobility operator or the user.

Several group signature schemes exist using different cryptographic calculations. Implementations exist for the ACJT [5] and the CG [18] group signature schemes [100]. The performance has been analyzed and compared in [31, 34]. The ACJT scheme is proven secure and coalition resistant under the strong RSA and DDH (Decisional Diffie-Hellman) assumptions. Also the CG scheme is provably secure under the strong RSA assumption. Boneh et al. have developed a short group signature scheme [9] to reduce the signature size to be more suitable for low-resource environments, while offering the same amount of security. The POPCORN protocol should use the short group signature scheme, since the electric vehicle and charging station use low-resource hardware and multiple signatures generated and verified during a charging session.

5.2.3 The service detail record

According to the ISO/IEC 15118 protocol the charging station creates a service detail record with all the necessary information, so that the mobility operator can pay the energy provider. The ISO/IEC 15118 protocol does not specify the details of the service detail record. For the POPCORN protocol, the content of the service detail record has been specified. The charging station creates the SDR with the values it knows and includes the identifier of the energy provider encrypted with the payment intermediary's public key. The SDR is sent to the electric vehicle. The vehicle then appends its Contract ID and roaming status encrypted with the mobility operator's public key. All values appended by the electric vehicle are encrypted with the public key of the mobility operator, so that in case a less privacy-preserving version of the POPCORN protocol is used which sends the SDR via the charging station, the charging station cannot learn any additional details. All public key encryption must be probabilistic. The ISO/IEC 15118 standard has set the requirement that the electric vehicle shall not perform any encryptions, due to the electric vehicle's limited processing power. However, most low-cost and low-resource processors can perform (limited) cryptography. Also, for the anonymous credentials and group signatures the electric vehicle is required to perform some cryptographic computations. Hence, this requirement is abandoned for the POPCORN protocol. Finally, the EV signs the complete SDR. The vehicle's signature is included, so that if the vehicle cheats and includes someone else's Contract ID, the mobility operator can directly detect this. The mobility operator verifies the signature and compares the identity with the Contract ID. In addition, the signature can

be used for integrity protection. The SDR content is summarized in Table 5.1.

Field	Encrypted with public key of
Included by the charging station:	
Amount of electricity received	✗
Chosen tariff (if applicable)	✗
Amount payable	✗
EP identifier (Spot Operator ID)	Payment intermediary
Session/transaction number	✗
Appended by the electric vehicle:	
Contract ID	Mobility operator
Roaming status	Mobility operator
EV Signature over complete SDR	Mobility operator

Table 5.1: The content of a SDR for the POPCORN protocol.

It is not required that the SDR is transmitted to the mobility operator directly after charging. In fact, not sending it directly offers privacy-preserving benefits, since the mobility operator does not learn anything about the charging time. However, a payment period shall be defined by the eMobility system. This period sets a maximum time frame for outstanding bills. The electric vehicle is responsible to deliver the SDRs, so that the mobility operator has enough time to process the payment. If the payment period has passed and the energy provider did not receive any payment, the energy provider is entitled to dispute resolution.

5.2.4 EV to MO communication

The POPCORN protocol requires the electric vehicle to communicate with the mobility operator in two occasions: (i) contract establishment and credential updates and (ii) SDR delivery. For case (i) the communication has to be real-time, as the vehicle also expects a reply from the mobility operator. For case (ii) the electric vehicle only has to send data to the mobility operator and the timing requirements are less important. Both cases require the communication to be privacy-preserving and secure. Especially, case (i) requires an authenticated and secure channel, because the contract and group signature credentials are exchanged. For anonymous credential and group membership updates a privacy-preserving communication channel is not required, since the updates can be non-interactive and only the intended vehicle can apply the update.

The reason for requiring the electric vehicle to directly communicate with the mobility operator without using the charging station is to hide any visible content, the identity and the IP address of the mobility operator from the charging station. Equally, the mobility operator must not be able to deduce the charging location, based on the source IP address of the messages.

One approach is to use the electric vehicle user's home Internet connection. Since the mobility operator, knows where the user lives the source IP address does not reveal any new information about the user. The credential updates and SDR delivery can be conducted overnight while the vehicle is charging at the domestic charging spot. If the vehicle has access to the cellular network, that medium can also be used. Another approach is to use the charging station, if it can offer a private connection, e.g., using onion routing (TOR [95]) or via a privacy-proxy. A privacy-preserving Internet connection can also be used for other eMobility usecases, such as allowing the EV user to access the Internet while the vehicle is charging. Finally, a non-technical method is to legally prohibit the charging station/mobility operator from using the IP addresses to deduce the home/charging location. The latter approach requires the least changes to the eMobility infrastructure, but can be easily exploited.

The POPCORN protocol by default uses the EV user's home Internet connection, as this requires no changes to the charging stations and vehicles to be able to use privacy-preserving communication

means. An additional benefit is that the charging station can now operate completely offline during charging. The communication channel with the mobility operator has to be authenticated and secured, e.g., using TLS. For case (i) mutual authentication is required.

5.2.5 MAC addresses

The electric vehicle communication controller (EVCC) installed in every electric vehicle manages the communication with the charging station. Each EVCC received a unique MAC address from its manufacturer. When the electric vehicle is connected to the charging infrastructure, the EVCC obtains an IPv6 address, as specified in RFC 4291 [54], using Stateless Address Autoconfiguration (SLAAC). First, an interface identifier is generated from the MAC address of the EVCC [61]. This identifier is then appended to a prefix to form the vehicle's IPv6 address. Since by design the interface identifier is globally unique, the vehicle can be tracked based on the identifier and the generated IPv6 address. Privacy extensions for IPv6 have been developed [69] to address the privacy concerns related to MAC and IPv6 address. When privacy extensions are enabled, an ephemeral IP address is generated by concatenating a randomly generated host identifier with the assigned network prefix.

The POPCORN protocol requires the privacy extensions, as defined in [69], to be used be all electric vehicles.

5.3 The final protocol: POPCORN

This section introduces the final privacy-preserving protocol – the POPCORN protocol – including all steps: mobility contract establishment, EV charging authentication, and payment of charging expenses. Then, the POPCORN protocol is compared to the ISO/IEC 15118 standard. Since the POPCORN protocol is based on the ISO/IEC 15118 standard, it follows the message sequence, structure and general trust and security requirements, unless otherwise stated. Step 0 is only required when the EV user signs a new mobility contract. The steps 1-4 occur during every charging session. Step 5 is only required in case of disputes.

Step 0 a-g) Mobility contract establishment At vehicle production the OEM installs the Provisioning Certificate in the vehicle. The EV user then signs a mobility contract with her mobility operator and registers the vehicle with the mobility operator. Then, the mobility operator asks a global certificate authority to generates the anonymous credentials for the vehicle. Further, the vehicle has to create a secret key for the group signature scheme.

Before the first charging session using automated billing, the anonymous contract credentials and the group signature credentials have to be installed in the electric vehicle. The electric vehicle contacts the mobility operator for credential installation, using the home Internet connection of the EV user. The anonymous credentials including any other relevant contract attributes, e.g., special tariffs, are installed in the vehicle. To obtain the group membership certificate, the vehicle has to contact the group manager, i.e., the dispute resolver. Assuming that the electric vehicle can trust its mobility operator, the mobility operator can also obtain the group signature credentials for the vehicle and include it with the anonymous credentials installation. This reduces the (computational) efforts for the vehicle. Otherwise, the vehicle has to directly contact the dispute resolver to create and obtain the credentials. Now the electric vehicle can charge using the automated billing feature.

The contract establishment including the credential installation is illustrated in Fig. 5.11.

During credential updates (referred to as certificate update in the ISO/IEC 15118 protocol), the anonymous credentials and the group signature credentials are updated as described above. If necessary, the mobility operator may contact the vehicle to inform it about a necessary update, e.g., when the group keys have been changed. The charging station will refuse the signature and stop the charging session, if the vehicle has outdated group credentials. Most updates are non-interactive and can be downloaded by the vehicle when it has an online connection.

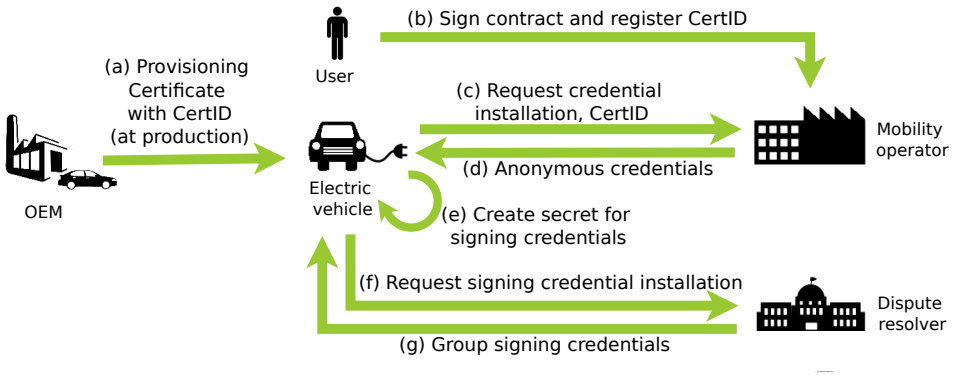

Figure 5.11: The POPCORN contract establishment.

Step 1) EV charging authentication When the electric vehicle is plugged into a charging station, the electric vehicle and charging station establish a connection as defined in ISO/IEC 15118. The ISO/IEC 15118 standard requires server-side TLS authentication to enable an authenticated and encrypted channel between the vehicle and the charging station as described in Section 3.4.3. Also the POPCORN protocol requires this. Next, for contract authentication, the electric vehicle proves to the charging station that it has a valid contract using its anonymous credentials. To show that the contract is still valid the vehicle can apply an attribute operation to compare the contract end date with the current date. The vehicle does not disclose any other contract attributes. The vehicle also has to proof that the anonymous credentials's validity period has not passed to show that the credentials have not been revoked. The charging station can locally verify the validity of the proof, and hence the charging contract. If the vehicle is eligible to special tariffs, the electric vehicle can use its credentials to prove this to the charging station. The vehicle can deduce its roaming status from the charging station's EVSE ID, since the identifier contains the energy provider's identifier. The electric vehicle does not inform the charging station about the roaming status.

Step 2) Charging loop with commitments During the charging loop the charging station sends the meter readings to the electric vehicle. The electric vehicle then generates a group signature over the readings and sends the resulting commitment back. The charging station verifies the signature with the group's public key. If the signature is valid the charging cycle continues, otherwise the charging station aborts the charging session. At the end of the charging session, the charging station forwards the group-signed commitments to the energy provider.

Step 3) SDR delivery and payment At the end of the charging session, the charging station generates the partial SDR and sends it to the electric vehicle. The electric vehicle then appends its Contract ID and roaming status, and signs the complete SDR. For the POPCORN protocol, it is assumed that the vehicle does not cheat about its roaming status. To prevent the cheating risk the approach described in Section 5.2.1 can be used.

When the electric vehicle has access to the user's home Internet connection, the SDR is submitted to the mobility operator. The mobility operator verifies the signature and uncovers the Contract ID and roaming status. The mobility operator now knows which user the bill belongs to and can inform and bill the user for the charging session. If the vehicle was roaming, the mobility operator may add additional charges.

In order to complete the processing of the SDR, the mobility operator sends the payment with the encrypted energy provider value and the transaction number to the payment intermediary. The payment handler decrypts the identity of the energy provider and forwards the payment and transaction number accordingly. Finally, the payment intermediary sends a receipt to the mobility operator, to confirm the payment.

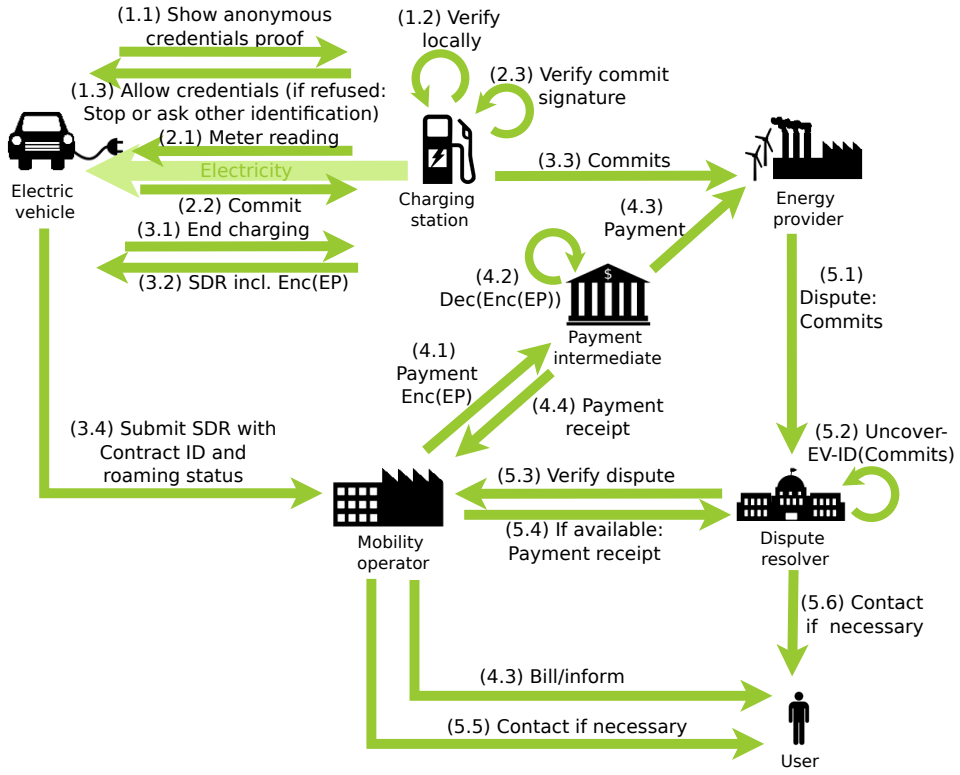

Figure 5.12: The POPCORN protocol for charging with automated payment.

Step 5) Dispute resolution If the payment of a charging session does not arrive within the defined payment period, the energy provider can contact the dispute resolver with the group-signed meter reading. The dispute resolver has access to the group's secret key and can uncover the vehicle's identity. As a first step, the dispute resolver contacts the mobility operator of the vehicle in questions and requests the payment receipt. If the mobility operator cannot send the receipt the dispute resolver may instruct the mobility operator to get in contact with his customer or the customer is contacted directly. The dispute is resolved when the a valid receipt for the transaction in question is shown to the dispute resolver.

The POPCORN protocol steps 1-5 are depicted in Fig. 5.12.

5.3.1 The comparison of the protocols

Next, the POPCORN protocol is compared with the ISO/IEC 15118 protocol. This comparison is meant to give an overview of the different approaches used for the charging protocol steps. Table 5.2 lists the differences in the credentials used. The charging protocol steps are compared in Table 5.3. For a more detailed analysis of the privacy properties and the overall evaluation of the POPCORN protocol see Section 6.1.

Usage	ISO/IEC 15118	POPCORN
Contract authentication	Certificate and Contract ID	Anonymous credentials with contract attributes, incl. Contract ID
Tariffs	Contract ID or attribute certificate	Anonymous credentials attributes
Meter reading commitment	Signing key	Group membership certificate and secret member key

Table 5.2: Comparison of the credentials and keys of the ISO/IEC 15118 and POPCORN protocol.

Scenario	ISO/IEC 15118	POPCORN
Contract establishment	Provisioning Certificate registered with mobility operator.	Same
Credential installation/ update	EV obtains: Contract Cert. and ID, *CRLs*	EV obtains: Contract anonymous credentials, Contract ID, group membership certificate
Contract authentication	EV shows Contract Cert. and ID, CS verifies with backend	EV proves contract validity with anonymous credentials, CS verifies locally
Meter reading commitment	EV signings with its signing key, CS can verify signature, sent to EP	EV generates group signature, CS can verify signature, sent to EP
SDR delivery	CS generates and delivers SDR	CS generates partial SDR, EV appends extra values, signs and delivers SDR
Payment	MO reads SDR and pays EP	MO reads SDR and sends payment and encrypted receiver value to PH, PH decrypts receiver and forwards payment, PH sends receipt to MO
Dispute	EP uncovers EV identity from signature and contacts EV/MO	EP submits dispute with DR, DR verifies and uncovers EV identity from group signature, DR contacts MO/EV and obtains payment receipt to resolve dispute

Table 5.3: Comparison of the ISO/IEC 15118 and POPCORN protocol steps.

5.4 Summary

This chapter presented our privacy-preserving charging protocol POPCORN. The development of the POPCORN protocol has been described as the step-wise modifications of the ISO/IEC 15118 protocol based on the suggestions of Chapter 4. Next, the concrete technologies used to realize the abstract POPCORN have been explained and the final POPCORN protocol has been presented. Finally, the designs of the ISO/IEC 15118 and the POPCORN protocol were compared.

To evaluate the POPCORN protocol with respect to privacy and feasibility, the next chapter will conduct a privacy impact assessment of the POPCORN protocol as part of the theoretical discussion. For the practical evaluation, a proof-of-concept is implemented based on the protocol description in Section 5.3 and the technologies discussed in Section 5.2.

CHAPTER 6
Evaluation

In this chapter our privacy-preserving charging protocol – POPCORN – is evaluated with respect to privacy and feasibility. The protocol evaluation is split in a theoretical and a practical part. As part of the theoretical evaluation, the PIA developed in Chapter 4 is applied to the POPCORN protocol in the same manner as it was done with the ISO/IEC 15118 protocol. For the practical evaluation, a proof-of-concept is developed. The implementation is described in Section 6.2. Finally, the chapter concludes with an overall discussion of the POPCORN protocol, and the trade-offs between privacy protection and effort.

6.1 Theoretical evaluation: PIA of the POPCORN protocol

Since the privacy properties of the ISO/IEC 15118 protocol has been evaluated with a privacy impact assessment, the POPCORN protocol is also evaluated with a PIA. This allows for comparison of the two assessments.

Systematically evaluating and proving privacy is a complex task. Privacy is not all provable cryptography, but it often contains hidden information flows and unforeseen loopholes, such as monetary information flows and covert channels. For example, even though two parties do not reveal any secret information to each other, knowing about each other's IP address can pose a privacy risk.

In the following, the PIA of the POPCORN charging protocol is conducted. The assessment uses the approach proposed in Section 4.2.1.

6.1.1 Scope and purpose definition

This privacy impact assessment analyzes the POPCORN eMobility system, as described in Section 5.3. As for the PIA of the ISO/IEC 15118 protocol (see Section 4.3), the focus is on the privacy protection of the electric vehicle user and the contract-based charging scenario. The purpose of this assessment is to evaluate the privacy-preserving properties of the POPCORN protocol.

6.1.2 Stakeholders

The stakeholders of the ISO/IEC 15118 protocol PIA have been addressed in Section 4.3.2. For this privacy assessment we will concentrate on the new stakeholders of the POPCORN charging protocol. The description of the **electric vehicle user**, **charging station**, **CS's energy provider**, and **EV's mobility operator** remain unchanged. The two additional stakeholders and their roles with respect to the POPCORN protocol are explained.

Dispute resolver (DR) The dispute resolver is a trusted party of the POPCORN eMobility system. The DR is the group manager for the meter reading commitment credentials. The tasks include managing the joining and leaving of group members and distributing the keys for signing the meter reading commitments. The electric vehicle may have to contact the DR to obtain its signing

credentials, but this may also be initiated by the vehicle's mobility operator The dispute resolver is contacted by the energy provider in case of disputes about outstanding payments. The DR verifies the dispute and may uncover and contact the concerned mobility operator and electric vehicle.

Payment intermediary/handler (PH) The payment handler is used to handle the monetary flow between the mobility operator and the energy provider. The PH receives the charging payment from the mobility operator and sends it to the rightful energy provider. The stakeholders trust the PH to deliver the payment correctly.

The clearing house described in the ISO/IEC 15118 protocol is no longer required to support the message exchange in the backend. It may be able to assist with other tasks, e.g. as payment handler, assuming it is a trusted party. Allowing more than one payment handler reduced the risks of becoming a bottleneck or a single point-of-failure.

6.1.3 Information assets

In the same manner as for the ISO/IEC 15118 protocol, the messages of the POPCORN protocol are inspected for important information assets. Table 6.1 summarizes the findings. The assets found in the ISO/IEC 15118 protocol are included in the table for easy comparison. The text printed in italics marks parts that are identical with the ISO/IEC 15118 protocol findings.

Asset name	Origin	Use(s)	Lifetime	Issue(s)
Provisioning certificate, Cert ID	*Installed by OEM in production process.*	*Used to link vehicle to mobility contract when concluding a mobility contract. Not used for charging communication.*	*Lifetime of the vehicle.*	*Unique for each vehicle.*
Anonymous contract credentials	*Created by a certificate authority. Obtained from MO.*	Allows EV to prove it has a charging contract. *EV sends (attribute) proofs to CS for (contract-based charging) authentication.* CS verifies proofs locally.	*4 weeks - 2 years*	Unique for each vehicle-contract. Actual credential not disclosed.
Contract ID [35, 50]	*Obtained from MO.*	*Ties vehicle to charging contract.* EV appends it (encrypted) to the SDR to identify its contract to the MO.	*4 weeks - 2 years*	*Unique for each vehicle-contract. Reveals the origin country and mobility operator of the contract*, but is only disclosed to the MO.
Attribute certificate	Not used in POPCORN. Attributes can be included the the anonymous contract credentials.			
Identity certificate	Not used in POPCORN.			
Customer ID	Not used in POPCORN.			
EVCC ID	Installed during manufacturing of EVCC component.	*The EV's identifier. Contains the MAC address of the EVCC, used during session setup with the CS.* Randomized according to [69].	Lifetime of the EVCC hardware.	The MAC is randomized.
E-Mobility operator ID	Not used in POPCORN.			
EVSE ID [35, 50] and Power outlet ID	EVSE operator will fix the power outlet ID.	*Unique identification of the charging spot.* EVSE ID used by EV to determine roaming status.		*Identifies the charging location. EVSE ID reveals the CS's country and EP.* Only revealed to EV.

Asset name	Origin	Use(s)	Lifetime	Issue(s)
EVSE operator ID or Spot Operator ID (i.e. EP ID)		Included in SDR, but encrypted with payment intermediary's public key.		*Reveals the EP identity. May reveal approx. charging location.* Not sent with EV identifier.
Meter reading signing credentials	Created by EV and DR. Obtained from DR.	Used for creating group signature over meter readings.		Kept secret by EV.
Signed meter readings	EV generates group signature over the meter reading of the CS.	*Used as proof that the EV consumed the said amount of energy. CS sends it to the EP.*		DR can reveal EV identity, but identity only used by DR to settle the dispute.
Service detail record	Generated by CS at the end of the (charging) session. EV appends extra values.	Sent to MO by EV. Contains information, so that MO can inform/bill EV user and MO can pay EP via PH.		Reveals EV identity (Contract ID) to MO. PH learns MO and EP, but not EV or CS.
Timestamps	*Added by CS to specific ISO/IEC 15118 messages.*	*Used during SessionSetupRes, for MeterInfoType and PaymentDetailsRes messages.*		CS does not sent timestamped messages to backend containing visible EV identifiers.
Roaming status	Added by EV to the SDR.	Used by the MO to charge the EV user roaming fees.		The MO learns whether the EV charged at a charging station operated by the MO or at another EP's charging station.

Table 6.1: Identified information assets of POPCORN. The italic text marks parts that are identical to the ISO/IEC 15118 protocol. (continued)

How the certificates and identifiers are linked is illustrated in Fig. 6.1.

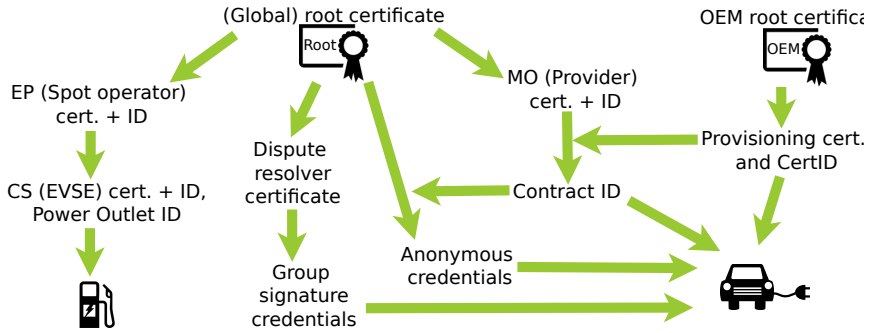

Figure 6.1: The links between the certificates and identifiers for the POPCORN protocol.

The next step is to analyze which of the information assets listed in Table 6.1 are personally identifiable information, i.e., which assets uniquely identify the electric vehicle and hence the user. The following assets identify the EV:

- Contract ID
- Anonymous contract credentials
- EVCC ID
- Signed meter readings (only towards DR; DR can link EV to EP and MO)
- Service detail record with appended EV data (only towards MO; MO cannot link EV to CS/EP)

Further, the roaming status is critical. If the vehicle is not roaming, the mobility operator knows that the vehicle used one of his own charging stations or one with which the mobility operator has a no-roaming-fee contract.

6.1.4 Information requirements and use

Next, the POPCORN's steps are considered in more detail to examine the usage of the information assets, especially the personally identifiable information assets. The minimum information requirements and the actual information usage are compared. The analysis considers the communication for the (i) mobility contract establishment, (ii) EV authentication and (iii) charging payment including dispute resolution. in these scenarios.

Mobility contract establishment During contract establishment, the vehicle obtains all required credentials and keys to be able to use contract-based payment for charging. A detailed description can be found in Section 5.3 Step a-d. Figure 5.11 illustrates the procedure.

The information requirements are summarized in Table 6.2. The ISO/IEC 15118 protocol (taken from Table 4.2) is included in the table for comparison.

Scenario	Actual intent	ISO 15118	POPCORN	Min. required
Creating the contract.	Creating the contract.	– (legal issue)	– (legal issue) Provisioning Certificate is registered with MO (offline).	– (legal issue) Provisioning Certificate needs to be registered with MO (offline).
Link EV to contract, to show charging contract capability.	Give the EV method to prove that it will pay for the charging expenses.	Provisioning certificate to obtain contract certificate and ID.	Provisioning certificate to obtain anonymous credentials.	Contract does not need to be linked to a vehicle identifier. The vehicle only needs a proof that it has a valid contract.

Table 6.2: Mobility contract establishment – ISO/IEC 15118 and POPCORN compared.

Both the ISO/IEC 15118 and the POPCORN protocol link the vehicle to the mobility contract. It is also possible to link the contract to a pseudonym that the vehicle knows. During the contract establishment the vehicle uses the pseudonym to obtain the contract credentials.

EV contract authentication To show the vehicle has a valid charging contract, it creates a zero-knowledge proof with anonymous contract credentials. The actual anonymous credentials are not sent to the charging station. The charging station verifies the proof locally. This procedure is described in more detail in Section 5.3 Step 1. Figure 6.2 shows the POPCORN contract authentication.

The information requirements are summarized in Table 6.3. The ISO/IEC 15118 protocol (taken from Table 4.3) is included in the table for comparison.

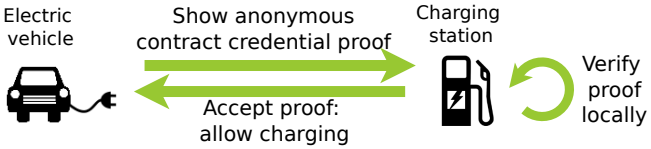

Figure 6.2: The information exchanged for charging contract authentication according to the POPCORN protocol.

Scenario	Actual intent	ISO 15118	POPCORN	Min. required
EV shows it has a charging contract.	CS knows EV has a valid charging contract.	Contract certificate, contract ID and MO ID have are sent to CS.	Anonymous credential proof with contract end date attribute operation.	A proof that the EV has a valid contract is enough. Not necessary to include MO identifier (can be derived from Contract ID/Certificate).
Online CS/real-time validation:				
CS validates the contract details.	CS is convinced contract is valid.	Contract ID, MO ID, CS operator ID and power outlet ID are all send to backend, i.e., the MO.	CS verifies the proof locally.	Not necessary to include CS identifiers when contacting backend. Validation can be done offline.
Offline/semi-online CS:				
CS validates the contract details.	CS is convinced contract is valid.	Information may still be sent to backend when CS is online, or user interaction is required (e.g., entering a PIN).	CS verifies the proof locally.	Not necessary to include CS identifiers when contacting backend. Validation can be done offline.

Table 6.3: EV contract authentication – ISO/IEC 15118 and POPCORN compared.

For the POPCORN protocol it is not necessary to use the backend for contract credential verification. The contract proof can be verified offline at the charging station. In addition, if the charging station cannot verify the proof, it is possible to contact a certificate authority in the backend, without making the contract authentication privacy-invasive.

Charging payment including dispute resolution After charging, the charging station sends the signed meter readings to the energy provider and a SDR to the electric vehicle. The electric vehicle appends extra information to the SDR and submits it to the mobility operator. The content of the SDR is defined in Section 5.2.3. The mobility operator has all the information to inform/bill the EV user for the charging session and to pay the energy provider. The payment is handled by a payment intermediary, so that the mobility operator does not learn the identity of the energy provider. These steps are described in more detail in Section 5.3 Step 2-5 and illustrated in Figure 5.12.

The information requirements are summarized in Table 6.4. The ISO/IEC 15118 protocol (taken from Table 4.4) is included in the table for comparison.

The group signature on the meter readings hides the identity of the vehicle from the charging station and the energy provider. If there is a dispute the dispute resolver has the means to uncover the identity.

6.1.5 Information handling and other considerations

The POPCORN protocol itself does not state any information handling requirements. However, the amount of personally identifiable information that can be collected about the EV user has drastically been reduced by design. We shall briefly consider how the POPCORN protocol fulfills the privacy

Scenario	Actual intent	ISO 15118	POPCORN	Min. required
Send the signed meter readings to the EP.	Show the EP which EV has consumed energy. Give EP a means to prove the energy consumption in case of dispute.	Meter readings signed by EV are sent by the CS to the EP.	Group signature on meter readings.	CS can send otherwise authenticated meter readings.
Send the SDR to the MO.	Tell the MO about the charging expenses for paying EP and informing/billing EV user.	SDR created by CS and sent by the CS to the MO.	SDR created by CS/EV, EP name is encrypted with PH's public key and submitted by EV to MO.	Bill or signed meter readings. Not necessary to use CS to forward the bill.
Payment of the EP by MO.	MO has to pay the EP.	SDR contains enough information. Details unspecified.	MO sends the payment with encrypted EP identifier to PH, who pays EP and sends receipt back to MO.	MO has to know whom to pay (not if it goes via PH), how much to pay and which EV user to charge.

Table 6.4: Charging payment – ISO/IEC 15118 and POPCORN compared.

requirements, as discussed in Section 4.1.1. While most of the requirements are of legal nature, some requirements may be fulfilled by the technical design of the POPCORN protocol.

1) Purpose specification Most stakeholders of the eMobility infrastructure cannot record personally identifiable information about the EV user, only the mobility operator and the dispute resolver. The mobility operator records personally identifiable information about the charging sessions in order to inform and bill the user for the charging expenses. Further, the dispute resolver can record personally identifiable information about the EV user, i.e., it knows the energy provider, the mobility operator and the electric vehicle identity. Besides requiring this information for dispute resolution, the dispute resolver may want to keep a record of past disputes for a defined period of time to be able to detect vehicles that frequently cause disputes. Frequent disputes may be caused by faulty vehicle hardware, for example, causing the SDR delivery to fail. The dispute resolver may also want to keep a list of electricity providers that request dispute resolution to detect if one of them tries to cheat the eMobility system.

The purpose specification is mainly a legal task. The mobility operator is the only stakeholder in direct contact with the EV user and has to inform the user during the legal contract establishment. The purpose should be defined in the mobility contract.

2) Consent The EV user has to give her consent to the collection and use of her personally identifiable information data. Similar to the purpose specification, this should be addressed during contract establishment.

3) Limited collection The POPCORN protocol limits (by design) the amount of data that can be collected about the EV user to the minimum required. Whether the payment intermediary is allowed to collect any information about the payment transactions has not been defined. However, it does

not relate to the EV user, since the payment intermediary only sees the monetary links between an energy provider and a mobility operator.

4) Limited use The use of personally identifiable information has to match with the purpose specification. For example, the dispute resolver may only use his abilities to uncover the electric vehicle identity for the purpose of following up on a dispute, but not to inform the energy provider about who was charging at which charging station.

5) Limited disclosure Information collected about the EV users is only allowed to be disclosed to those parties that require it. Overall, the POPCORN protocol already distributes the required information to the rightful entities. There is no need for additional information disclosure. Further, no stakeholder is allowed to make his information available to other stakeholders. For example, during dispute resolution the dispute resolver may not forward the uncovered EV identity to the energy provider. The dispute resolver is responsible for settling the dispute.

6) Limited retention Any collected information may only be kept for a set period of time. In some cases the legislation may define a minimum period of time for accountability, especially when monetary transaction are involved, e.g. the mobility operator billing the EV user. Otherwise, the retention period shall be defined in the mobility contract.

7) Accuracy Any data collected by the eMobility system has to be accurate. The mobility operator, for example, may not tamper with the charging bills. Since the electric vehicle signs the SDR, the POPCORN protocol prevents this and and prove that the bill was tampered with.

8) Security Since the POPCORN protocol is based on the ISO/IEC 15118 standard, it makes use of the same security mechanisms. The communication channels are encrypted (TLS) and any personally identifiable information information is in most cases encrypted, e.g., the Contract ID in the SDR. The storage of credentials and keys in the vehicle has to be secure. Equally, the dispute resolver and mobility operator and any certificate authority have to protect their collected data and any credentials/keys.

9) Openness The EV user has to right to inspect her information at any time. By default the mobility operator informs the EV user about each charging session. The dispute resolver may also be asked by the EV user to show which information it has stored about the user.

10) Compliance Overall the POPCORN protocol and the eMobility infrastructure have to comply with legal regulations and fulfill their contracts. For example, the mobility operator has to fulfill his duty to pay the energy provider for the charging expenses of his EV customer.

6.1.6 Evaluation

The goal of the POPCORN protocol is to offer complete privacy-preserving charging while using a mobility contract for payment. The protocol was designed to be privacy-preserving using technical means.

The personally identifiable information assets were examined in Step 3 of the PIA (see 6.1.3). While there still exist personally identifiable information assets, the use and disclosure has been limited. The privacy-invasive Contract ID is only used by the electric vehicle to inform its mobility operator about which vehicle has been charging, so that the mobility operator can inform and bill the EV user. The EVCC and MAC address are no longer used to create the IPv6 address of the vehicle, so that the charging station cannot link two charging sessions of the same vehicle. Also, the signed meter readings no longer reveal the electric vehicle identity to the charging station or energy provider.

PIA step 4 has analyzed the information requirements (see 6.1.4). Contract verification with the backend is no longer required and if it is used it is privacy-preserving, due to the design of the contract authentication proof. The monetary information flow has been hidden, offering more privacy than the PIA suggestion. All PIA recommendations for minimizing the information use have been implemented in the POPCORN.

The information handling and compliance with the privacy requirements has been discussed. Most requirements are fulfilled by the design of the POPCORN protocol. The remaining privacy requirements are outside the scope of the protocol and can be determined during the implementation of the system. Some requirements may be defined as part of the mobility contract, such as the purpose specification or the date retention period.

The privacy-invasions summarized in the ISO/IEC 15118 PIA have been reduced. There are no longer any privacy invasions of type 2. A PIT 1 occurs when the EV shows its identity in the charging bill. This is unavoidable for the use of a charging contract. The mobility operator has to be informed which EV customer to inform and charge. Dispute resolution results in a PIT 3 and 4. The dispute resolver learns the EV identity together with the mobility operator (PIT 3) and the energy provider identity (PIT 4). For accountability and abuse protection this cannot be prevented. Here it is important that the dispute resolver is a trusted party that does not collude with any of the other stakeholders, e.g., an energy provider. It is possible to avoid the PIT 4, by requiring the energy provider to submit the dispute anonymously. Then the dispute resolver only learns that the vehicle is a customer of some mobility operator. However, using this approach means that the dispute resolver is not able to detect abuse of the dispute resolution feature, e.g., an energy provider that request dispute resolution for every charging session. While this form of abuse does not offer any benefits to the energy provider, it can be considered a form of a denial-of-service attack on the dispute resolver. Further, the payment intermediary learns about mobility operator to energy provider links, however without any EV identifier. Hence, this does not result in any privacy-invasion. Nevertheless, the payment intermediary has to be a trusted party that will handle the payment correctly. Further, the roaming status (included in the service detail record) reveals information about whether the vehicle used a charging station operated by another energy provider or one of the mobility operator's charging stations. However, the mobility operator cannot link the charging commits to the service detail record. Hence, the mobility operator does not learn which exact charging station has been used. Unless the mobility operators are willing to abolish roaming fees, including the roaming status cannot be avoided.

The PIA applied to the POPCORN protocol shows that the protocol is privacy-preserving and the ISO/IEC 15118 PIA recommendations were applied. However, as for any protocol, it is important that all credentials and key material is kept secret. The vehicle has to protect its anonymous credentials and group singing key, and these credentials have to be securely transferred to the vehicle. In addition, the mobility operator may not be the issuer of the anonymous credentials, because the issuer is revealed during the contract authentication proof. A certificate authority on behalf of the mobility operator has to issue the credentials. Preferably, the certificate authority is a large global organization responsible for a large part of the eMobility infrastructure. Since using small certificate authorities to issue the anonymous credentials will reduce the size anonymity set size.

6.2 Practical evaluation: Proof-of-Concept

In order to evaluate the feasibility of the POPCORN, a proof-of-concept has been implemented. This section discusses the implementation setup, the tested scenarios and the results.

6.2.1 Scope, purpose and limitations

The proof-of-concept is a small demonstration of the POPCORN protocol and tests several scenarios, including dispute resolution. The implementation analyzes the practicality of the POPCORN

protocol and examines whether the protocol description is complete and detailed enough to implement the charging protocol. Further, the proof-of-concept includes a small electrical toy car and a self-made charging station, to physically demonstrate the protocol and charging scenarios. Both the electric vehicle and the charging station use low-resource hardware to simulate the real-life hardware conditions.

The implementation focuses on the POPCORN protocol steps and uses the ISO/IEC 15118 protocol as foundation. As the POPCORN protocol design, the proof-of-concept considers the charging scenario with automated billing of a single vehicle and the communication between the electric vehicle, the vehicle's mobility operator, a charging station and the charging station's energy provider. A dispute resolver who is the group manager for the group signature scheme and a payment intermediary who forwards the payment is also implemented. A certificate authority used to distribute keys, certificates and to issue the anonymous credentials is not implemented. The stakeholders generate and distribute their keys themselves before the actual POPCORN protocol run. The mobility operator issues the anonymous credentials, however, in a real-life implementation a large certificate authority shall issue the anonymous credentials as discussed in the PIA in Section 6.1.6. The offline mobility contract signing and registration of the vehicle's Cert ID with the mobility operator is outside the scope of the protocol. The electric vehicle identifier is registered with the mobility operator before the POPCORN protocol run.

The proof-of-concept does not implement any of the security mechanisms discussed in the ISO/IEC 15118 protocol, e.g. unilateral TLS authentication and encryption, since the focus is on the privacy implementation. The communication between all stakeholders uses TCP/IP and no other protocols, such as DLMS/COSEM, are used.

6.2.2 Software setup

The proof-of-concept is implemented using the Java OpenJDK [72]. The six stakeholders are implemented as separate Java processes. All stakeholders operate TCP servers and can also start outgoing connections. The electric vehicle only acts as client. All communication exchanges consist of one or more request-response pairs. A simple message structure has been defined, consisting of a message identifier, which specifies the purpose of the message, such as "SDR Delivery" and a data body, which may be empty or contain an undefined number of relevant data, e.g. a meter reading.

Anonymous credentials - Idemix The Identity Mixer (Idemix) system has been developed as part of the PRIME and PrimeLife research projects [77] and offers a Java implementation. The library is fairly complete and has already been used for other prototype implementations [56]. The libraries architecture is suitable for a distributed implementation, such as the POPCORN system. The issuer of anonymous credentials, the prover and the verifier roles can easily be taken by different stakeholders. The resources, e.g., the credentials or proofs, are encoded using XML and can either be send as part of a message or are accessible via URIs.

Small implementation-related edits were applied to make the library suitable for the proof-of-concept's communication exchange. Further, an additional feature was added to be able to compare a date that is included in a credential with the current date. To do so the proof specification parser was updated to fill in the current date for the `CURRENT_DATE` variable when parsing the inequality proof. This feature is required to check whether the charging contract is valid at the point in time when the vehicle wants to charge, i.e., the expiration date of the contract has to be larger than the current date.

For credential revocation "epochs" are used as described in [19, 88]. Epochs define the validity period of the credential independent of the expiration date of the contract and can be set to, e.g., a week or a month. The anonymous credentials has to be updated when the epoch changes. Using epochs as revocation methods reduces the strain on the vehicle of having to compute a proof that its credentials have not been revoked. When the epoch expired, the credentials can be updated overnight while the vehicle is not in use.

For the implementation the default parameters were chosen and no optimizations have been applied. However, special implementation for low-resource environments are being developed, as discussed in Section 5.2.1.

Group signatures - Camenisch-Groth Algorithm The short group signature scheme developed by Boneh et al. does not offer a Java implementation. However, a Java library exists for the Ateniese-Camenisch-Joye-Tsudik (ACJT) and the Camenisch-Groth (CG) group signature schemes [100]. The implementation is described in [31]. The library also offers tools to compare the speeds of the two algorithms. As also found in [31] the CG implementation is the faster one. Therefore, for the proof-of-concept the CG algorithm is used.

The library is in an experimental state and is less complete than the Idemix library. For deployment in the distributed POPCORN protocol where the group manager, the signer and the verifier are different stakeholders a few additional features were implemented, such as making certificates and keys persistent over program runs and allowing them to be included in the simple message structure defined for the proof-of-concept.

Charging/LEDs - Pi4J The proof-of-concept uses general purpose input/output (GPIO) pins to turn on a LED to visually indicate the active communication link between the toy car and the charging station. Further the GPIO pins are used to charge the toy car's batteries during the power delivery phase. To program the GPIO pins the Java library Pi4J is used.

6.2.3 Hardware setup

The proof-of-concept hardware setup is depicted in Fig. 6.4. The electric vehicle and the charging station processes are each run on a Raspberry Pi computer. A Raspberry Pi is a credit-card-sized computer which uses a 700 MHz ARM11 processor and supports the ARMv6 instruction set [78]. This single-board computer was chosen, because it can be fitted into a toy electric car for the physical demonstration of the charging protocol. Further, it has GPIO pins, which can be used to indicate the connection status, the status of the power delivery and to actually charge the toy car's batteries. Finally, the Raspberry Pi has a low-resource processor which more closely resembles the low-resource hardware of the electric vehicle's or charging station's communication controller. The backend processes are run on a Dell Inspiron 6400 laptop.

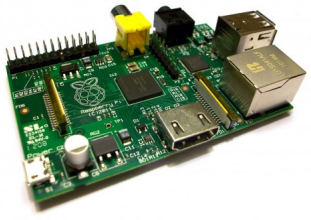

Figure 6.3: The Raspberry Pi computer [78].

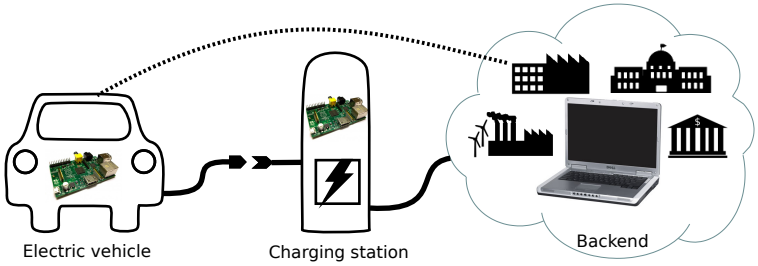

Figure 6.4: The proof-of-concept hardware setup.

All stakeholders are on the same subnet and are connected to each other via Ethernet. The electric vehicle additionally have a wireless networking adapter to contact the mobility operator and dispute resolver for credential and certificate installation and updates. During the charging session the electric vehicle and the charging station are connected to each other with a modified Ethernet cable. The cable has been fitted with a custom plug and uses only two wire pairs of the four-pair

Ethernet cable for 100 Mbps Ethernet communication. The other cables are used for charging and for detecting the physical connection between the charging station and the electric vehicle.

6.2.4 The scenarios

The following scenarios were tested with the proof-of-concept:

1) Normal charging First the anonymous credentials and membership certificate are installed/updated. Then a normal charging session with subsequent SDR delivery and payment is performed.
2) Expired contract The mobility operator installs expired contract credentials and the electric vehicle tries to charge at the charging station.
3) Cheating EP After a normal charging session, the energy provider request for dispute resolution for an already paid SDR.
4) Cheating EV During the charging session the electric vehicle disconnects the charging cables and leaves.

Next, for each scenario we will explain the steps in more detail and the resulting findings.

1) Normal charging

The normal charging scenario starts with the electric vehicle contacting the dispute resolver in order to join the group of vehicles. The dispute resolver is the group manager and generates a membership certificate for the electric vehicle. The electric vehicle stores the membership certificate locally on its storage device.

Next, the vehicle contacts its mobility operator for credential installation. The mobility operator generates the anonymous credentials and fills in the content. The credential structure is illustrated in the code listing below.

```
...
<Attributes>
        <Attribute issuanceMode="known"  name="credType"    type="string" />
        <Attribute issuanceMode="known"  name="contractID"  type="string" />
        <Attribute issuanceMode="known"  name="flatrate"    type="int" />
        <Attribute issuanceMode="known"  name="expDate"     type="int" />
        <Attribute issuanceMode="known"  name="epoch"       type="epoch" />
</Attributes>
<Features>
        <UpdateSpecification>http://www.issuer.org/UpdateSpec_Contract.xml
        </UpdateSpecification>
</Features>
...
```

The anonymous credentials contains five attributes. The first one declares the credential type and is set to "Charging contract". The second attribute lists the Contract ID. The third attribute shows if the vehicle has a flat-rate contract and can otherwise be used to denote the vehicle's tariff class. The forth attribute is the contract's expiration date encoded in unix-time and the final attribute is the epoch value that is used to limit the lifetime of the credential. The update specification declares that the last two attributes can be updated. The electric vehicle stores its contract credential locally.

Now the electric vehicle is ready to charge. The electric vehicle is connected to the charging station and the charging session begins. The active communication link is indicated with a turned on LED on the charging station. First, the ISO/IEC 15118 protocol messages for service discovery and service and payment selection are exchanged. For the proof-of-concept the vehicle always uses the DC charging option and the contract payment method. Then the contract authentication starts. The charging station sends a nonce and the vehicle creates the proof that the contract is valid. All attributes except the first one remain hidden as depicted in the code listing below. The first attribute is revealed to test the feature.

```
...
<Declaration>
        <AttributeId name="id1" proofMode="revealed"   type="string" />
```

```
        <AttributeId name="id2" proofMode="unrevealed" type="string" />
        <AttributeId name="id3" proofMode="unrevealed" type="int" />
        <AttributeId name="id4" proofMode="unrevealed" type="int" />
        <AttributeId name="id5" proofMode="unrevealed" type="epoch" />
</Declaration>
...
        <Inequalities>
            <Inequality publicKey="http://www.issuer.org/public/ipk.xml"
                operator="geq" secondArgument="CURRENT_DATE">id4</Inequality>
                <Inequality publicKey="http://www.issuer.org/public/ipk.xml"
                operator="geq" secondArgument="CURRENT_EPOCH">id5</Inequality>
        </Inequalities>
 ...
```

The vehicle sends the proof to the charging station and the proof is verified by the charging station. The charging station only requires the proof specification and the public key of the issuer to verify the proof. If the verification succeeds the charging starts. A second LED shows that power is being delivered to the electric vehicle. During the charging loop the charging station sends meter readings to the electric vehicle. The vehicle signs the reading and sends the signature back to the charging station. Before continuing the charging station verifies if the signature is valid. Once the vehicle is done charging it signals this to the charging station. The charging station then generates the SDR and sends it to the electric vehicle. The electric vehicle can be disconnected from the charging station. The vehicle appends its Contract ID and the roaming status and sends the SDR to the mobility operator, who initiates the payment procedure. The payment it send to the payment intermediary with the encrypted energy provider identifier. The payment intermediary decrypts the value and forwards the payment to the energy provider. Finally, the mobility operator gets a payment receipt.

Findings One of the features of Idemix is that it is possible to hide attribute values from the issuer. For the proof-of-concept this is not required since the mobility operator is the one who decides the values. However, in a real deployment of the POPCORN protocol this can be used to hide the information from the certificate authority who issues the credentials on behalf of the mobility operator.

Further, the time it takes for the cryptographic operations to create the proofs, signatures and to verify them has been measured when running the all proof-of-concept processes on the laptop, and when running the electric vehicle and the charging station on the Raspberry Pis. The results are summarized in Table 6.5.

Computation	**Time taken in milliseconds**	
	Laptop	**Raspberry Pi**
Installing anonymous credentials	1500	35000 (35 sec)
Updating anonymous credentials	620 - 2000	5500
Installing membership certificate	100	850
Creating contract proof	950	105000 (1 min 45 sec)
Verifying contract proof	1050	90000 (1 min 30 sec)
Signing meter reading	70	8000
Verifying signature	72	8500

Table 6.5: Mobility contract establishment – ISO/IEC 15118 and POPCORN compared.

While most operations take a reasonable amount of time, creating the contract proof and verifying it takes a long time on the Raspberry Pis. One of the factors that significantly slows down these steps is the use of the Java Virtual Machine (JVM), which has to be run on both Raspberry Pis to run the proof-of-concept. Modular exponentiation is one of the most costly operations used during the cryptographic computations and the calculations involve large integer values. The speed

of cryptographic operators using the default Java cryptography library and using native code within Java has been compared in [34]. The result shows that using optimized Java libraries already increases the speed of modular exponentiation by a factor of three. However, in a real deployment of the POPCORN system, no Java implementation is used. The entire vehicle and charging station computations will be implemented using native code that has been optimized for the low-resource hardware. Hence, the speed issues encountered in the proof-of-concept do not apply. The speed of installing and updating contract credentials and membership certificates is less important, because these operators can be done overnight while the vehicle is not in use.

Since a charging session generally takes at least a few minutes the time concerns should not affect the feasibility of the POPCORN protocol. Also, while the vehicle is generating the authentication proof the charging station can already determine the charging parameters. Equally, while the charging station is verifying the proof the vehicle can prepare the battery management module for power delivery.

2) Expired contract

For this scenario the electric vehicle first contacts the mobility operator for a contract credential update. The mobility operator creates an update which sets the contract's expiration date to some date in the past to simulate an expired contract. The vehicle then connects to the charging station. During the contract authentication phase, the electric vehicle tries to create the proof that it has a valid charging contract. However, because the contract is expired the proof cannot be created. The electric vehicle informs the charging station that it cannot provide a proof and the charging session is aborted.

Findings This scenario showed that the electric vehicle is not able to create a proof if the contract expired. Therefore, the contract authentication already fails on the vehicle's side and it is unlikely that a vehicle will approach the charging station with an invalid contract. To check if the contract is valid, the vehicle can generate a nonce itself and try to create a proof. If proof creation fails, the vehicle can inform the user that an Internet connection is required to update the credentials. However, depending on how the expiration date and the anonymous credentials itself are stored in the vehicle, it may be easier to simply check the expiration date in the contract credential.

Further, this scenario gave move insights into anonymous credential updates. During the anonymous credential installation the mobility operator informs the vehicle about the URI where the update will be published. The vehicle only needs to fetch the update from there and apply it to its existing anonymous credentials. This means that updating the anonymous credentials does not necessarily require contact with the mobility operator, given that the mobility operator already published the update and the vehicle knows the new values the update installs. The update is non-interactive. Since the epoch value increases by one with every new epoch the vehicle will know the new value. However, for contract expiration date updates the vehicle may need to be informed about the new value. The proof-of-concept implementation always contacts the mobility operator to make sure the update has been published and the vehicle knows the new values.

3) Cheating energy provider

For this scenario the energy provider is told to cheat, i.e., he starts a dispute request for an already paid charging session. After a normal charging session including payment, the energy provider contacts the dispute resolver with the last meter reading commit for dispute resolution. The dispute resolver uncovers the electric vehicle identity. Since the encoded identity is the vehicle's Contract ID the dispute resolver can easily deduce the mobility operator's identity, based on the format of the Contract ID. The dispute resolver contacts the mobility operator for verification. The mobility operator checks whether all SDRs for the given Contract ID have been processed and paid for. Since the bills are paid for, the mobility operator informs the dispute resolver and the dispute resolver informs the energy provider that the bill has been paid already. The dispute resolution is completed.

Findings This scenario showed a practical shortcoming of the POPCORN meter reading signatures and dispute resolution. The mobility operator has to check whether all his SDRs for the given customer have been paid. The energy provider and the mobility operator have no means to identify the specific charging session, so that it is possible to only check for one bill. Hence, the mobility operator also cannot send the payment receipt, since sending all payment receipts is infeasible. The dispute resolver has to believe the mobility operator the truthfully.

In addition, if the electric vehicle did not submit the bill, the mobility operator would respond the same, since the outstanding bill does not exist for the mobility operator. The system cannot distinguish a cheating vehicle from a cheating energy provider. To investigate the feasibility of the POPCORN dispute resolution process another scenario is tested.

4) Cheating electric vehicle

This scenario starts with a normal charging session. The vehicle's contract is accepted and the power delivery starts. During the charging phase, the vehicle unplugs the charging cable and leaves. The electric vehicle never received and forwarded the SDR. The charging station detected that the vehicle left and directly contacts the energy provider with the latest signed meter reading. The energy provider starts the dispute resolution procedure. The dispute resolver uncovers the identity and contacts the mobility operator. However, the mobility operator has never received a SDR for this charging session. The dispute cannot be solved.

A small change is made to the POPCORN protocol: When sending the signed meter readings, the charging station also sends the generated SDR to the energy provider. The SDR only contains the information known to the charging station, so there is no vehicle identifying information leaked to the energy provider. During dispute resolution the energy provider sends the commit and the SDR to the dispute resolver. Now the dispute resolver can forward the SDR to the mobility operator and ask for the payment receipt for that specific SDR. The SDR contains a transaction number (possibly the session ID) which makes it easy to search for the relevant payment, since the mobility operator also received the same transaction number in the SDR.

In this scenario the mobility operator notices that no SDR exists for the charging session in question and pays the bill using the SDR. The payment receipt is forwarded to the dispute resolver, who informs the energy provider that the bill has been paid. The dispute has been resolved. The mobility operator can charge the EV user using the Contract ID the dispute resolver uncovered.

Findings In order to solve this dispute a modification to the POPCORN protocol is required. The partial SDR that is created by the charging station also has to be sent to the energy provider with the commits.

By sending the partial SDR, the energy provider has the means to refer to a specific charging session and the mobility operator can quickly check for the payment receipt. The charging station or the energy provider can tamper with the SDR by increasing the amount of energy consumed. Hence, the dispute resolver should compare the meter reading value with the value stated in the SDR, before processing the dispute.

6.2.5 Evaluation

The proof-of-concept gives valuable findings on the feasibility of the POPCORN protocol. Overall the POPCORN protocol performs well and was able to handle all scenarios but the fourth scenario. As discussed, the time concerns can be solved by implementing the protocol using native code. The dispute resolution procedure had to be modified to be practical. The charging station has to send the commits together with the SDR, so that the energy provider has a means to relate to the specific charging session. This also makes it possible to let the dispute resolver forward the SDR when the vehicle failed to do so.

It is common for service records, invoices and the actual payment to contain a transaction number for accountability. The transaction number makes it possible to mark an outstanding invoice as paid

when the respective payment arrives. Therefore, also the payment should reference the transaction number. Then the energy provider can also detect if a payment is not correct, e.g. not enough was paid. Figure 6.5 illustrates the modified payment and dispute resolution procedure.

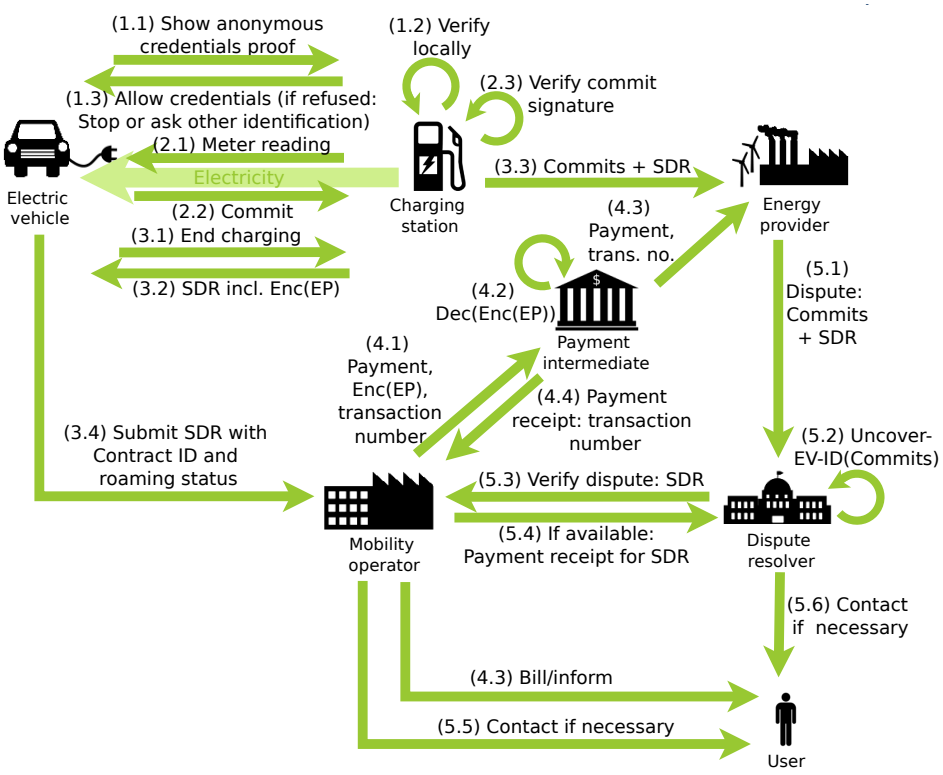

Figure 6.5: The improved POPCORN protocol for charging with automated payment.

However, in the case the electric vehicle is not roaming, i.e., when the mobility operator is also the energy provider, this the new POPCORN protocol can lead to privacy concerns. As depicted in Figure 6.6, the mobility operator receives the SDR from the vehicle and it also receives the commits and SDR from the charging station.

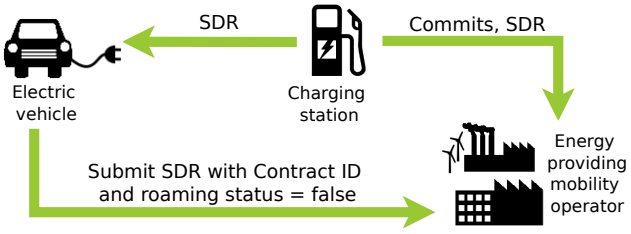

Figure 6.6: The backend messages of the POPCORN protocol when the mobility operator is also the energy provider.

If the mobility operator links the two SDRs the mobility operator does not learn anything new about the vehicle. Since the mobility operator knows the roaming status, he already knows that the vehicle used one of his own charging stations. However, if the mobility operator records which charging station delivered the commits and the SDR, the mobility operator learns the charging location of the EV user. This is a privacy invasion type 2 (see Section 4.3.6). To prevent this, the charging station can anonymously deliver the commits and SDR, e.g., by using a TOR connection, a privacy proxy or by using the Crowds protocol [79]. Then the mobility operator cannot relate the vehicle, i.e., the

user to a charging location. In addition, it is common that in large companies, such as a mobility operator who operates his own charging stations, the accounts receivable and the accounts payable are handled by different departments. Therefore, it is less likely that incoming SDRs of charging station and electric vehicle origin are matched with each other. Another option is to prohibit the matching of SDRs for the purpose of finding out the vehicle's charging location.

The proof-of-concept fulfilled its purpose of evaluating the POPCORN protocol in a practical manner. The implementation clarified the details of the dispute resolution and improved the protocol to offer better accountability.

6.3 Dicussion

The goal of the POPCORN protocol was to realize a charging solution, that is completely privacy-preserving by design and defines the entire charging communication, including the backend functions charging payment and dispute resolution. This has been achieved by the POPCORN protocol.

The user requirements of the eMobility system, discussed in Section 3.1, are fulfilled. A charging session requires no user interaction (Req. U1 & 2). After the cable is connected the vehicle handles the charging communication. The mobility contract is a convenient payment method (Req. U3). The POPCORN system takes into account that users want to roam (Req. U4). A non-partnered charging station only requires the proof specification and the issuer's public key to verify the contract proof. If necessary, the vehicle can transfer this data or the charging station can contact the backend if it has an online connection.

As given in the system requirements (see Section 3.1), the POPCORN protocol assumes a minimum trust relationship between the stakeholders (Req. S4). No party can learn the identity of the EV user and the exact charging location, i.e., which charging station was used, at the same time. The dispute resolver, the payment intermediary and a certificate authority are the only trusted parties of the POPCORN system. The other stakeholders trust them to perform their tasks truthfully. However, also these trusted parties do not learn enough information to know where a specific EV user has charged. The POPCORN privacy impact assessment discussed the privacy regulations in Section 6.1.5 and concluded that the POPCORN protocol fulfills them (Req. S3). Further, the electric vehicle is authenticated for all charging sessions, using the anonymous credentials (Req. S5). In case more specific authentication rules are necessary, more attributes can be added to the anonymous credentials. The accountability of the POPCORN protocol has been improved as a result of the proof-of-concept implementation (Req. S6). The practical evaluation also tested how the POPCORN protocol reacts to cheating participants (Req. S7). The protocol prevents cheating by design, e.g., the vehicle cannot append a wrong Contract ID to the SDR, because the SDR has to be signed by the vehicle. A mismatch between the signature and the given Contract ID will be detected. For other abuse cases, the dispute resolver can be contacted. Concerning the first system requirement (Req. S1), the POPCORN protocol has been based on the ISO/IEC 15118 standard, so that the least changes are required to the current IT infrastructure. The ISO/IEC 15118 protocol also makes use of a certificate authority to issue keys and certificates. In addition, the POPCORN infrastructure includes a dispute resolver and a payment intermediary. These two parties are required, to offer a complete privacy-preserving charging solution (Req. S2).

Finally, the theoretical evaluation of the POPCORN protocol confirms that POPCORN is a privacy-preserving charging system (Req. P1). The proof-of-concept tested the feasibility of the POPCORN protocol and shows that it can be realized in practice.

Further, the POPCORN protocol offers additional benefits beyond privacy protection. Since the contract proof is verified locally, it is not required that the charging station is online during the charging session. The charging station only occasionally needs to transfer the commits and SDRs to its energy provider. Further, the anonymous contract credentials can be extended to include tariff classes or other attributes for additional services. The mobility contract can also be used as payment methods for third party services. For example, charging spots may be installed on public parking places. The mobility contract can be used to automatically pay the parking fees.

While a full implementation of the POPCORN protocol offers the most privacy-preserving solution, this may not be desired by all stakeholders of the eMobility infrastructure. Some stakeholders, such as energy providers and mobility operators, benefit from the information they can collect about their services. For example, customer-specific offers can be made based on the user's charging behavior, or a mobility operator may want to start a roaming-partnership based on the roaming statistics of his customers. In addition, companies prefer transparency of their monetary transactions. If no payment intermediary is used, the mobility operator can bundle payments to the same energy provider, and no payment intermediary is required for transactions to the mobility operator's own accounts. Overall, some stakeholders may not be willing to invest the efforts required by the POPCORN protocol to technically protect the users' privacy. Here, efforts refer to the additional infrastructure, such as the payment intermediary, or the use of anonymous communication tunnels, to hide the origin of the data.

The POPCORN protocol has been designed in steps, where each step is a small modification of the ISO/IEC 15118 protocol and offers more privacy than the previous version of the protocol. The final result requires the most efforts, but offers a technical solution that is completely privacy-preserving. Due to the step-wise design of the protocol, it is possible to settle for a less privacy-preserving charging solution that requires less efforts. In addition, non-technical privacy protection can be applied to offer a similar level of privacy. However, a technical solution gives higher assurance than a non-technical solution. In the following we discuss, two less-effort variants of the POPCORN protocol.

The payment intermediary has been included to hide the monetary information flow between the mobility operator and the energy provider. When the payment intermediary is removed from the POPCORN protocol, the payment will link the mobility operator and the energy provider. However, only if the mobility operator or the energy provider is a small local company, the link will leak information about the place of residence or the charging location to the other. To prevent this privacy invasion, a non-technical regulation can be passed to prevent the use of this information for non-payment related purposes.

Another case that requires a change to the ISO/IEC 15118 protocol is the SDR delivery to the mobility operator. The goal is to hide the charging station and the mobility operator from each other. However, since the vehicle appends its Contract ID and roaming status in encrypted from, the charging station can see the final SDR without learning additional information about the electric vehicle. In order to deliver the SDR to the mobility operator, the electric vehicle needs an Internet connection. An online charging station can provide this. However, the privacy concern is that the IP addresses may reveal where the charging station and the mobility operator are located. Here, a non-technical privacy protection measure is to prohibit the use of such IP address records. Then, the electric vehicle is no longer required to use the EV user's home Internet connection for SDR delivery. Similarly, it may be prohibited to record which charging station delivered the commits and SDR to the energy provider, so that no anonymous delivery is required (see Section 6.2.5). Overall, prohibiting the use of IP addresses can drastically reduce the efforts required to protect the users' privacy, and hence lower the barriers to deploy the POPCORN protocol.

6.4 Summary

This chapter evaluated the POPCORN protocol, both theoretically and practically. For the theoretical evaluation, the privacy impact assessment that has been applied to the ISO/IEC 15118 protocol in Chapter 4 has been applied to the POPCORN protocol. The PIA concluded that the POPCORN protocol is privacy-preserving and gave suggestions for the credential issuance. A small demonstration has been designed for the practical evaluation. The implementation gave valuable insights into the practicality of the protocol and tested the protocol's response to two abuse scenarios. Based on the findings, the POPCORN protocol's accountability means have been improved.

Finally, the POPCORN protocol has been discussed in relation to the eMobility requirements

stated in Chapter 3. The discussion also addressed the efforts required to realize the privacy protection and considered non-technical protection mechanisms as alternative. The next chapter will conclude this thesis.

CHAPTER 7
Conclusion

The main objective of this thesis was to analyze the privacy impact of eMobility charging and billing communication, and to propose a completely privacy-preserving charging protocol that uses a mobility contract for payment. The proposed protocol has to be privacy-preserving by design. The ISO/IEC 15118 charging standard, which is currently being standardized, was chosen as the foundation for the privacy-preserving charging protocol, since the standard is likely to be adapted as the European charging standard and already defines the communication layers, the message structure and security measures.

In order to achieve the objective of this thesis, the first step was to define the eMobility infrastructure, based on the ISO/IEC 15118 standard and related work (see research question 1). The main eMobility requirements were gathered and the charging architecture has been summarized.

Since currently electric vehicle batteries have low ranges, it is proposed to re-charge the batteries whenever the vehicle is parked. Frequent charging sessions, offer opportunities for detailed tracking of the vehicle users if user-specific information is exchanged during a charging session. The next step was to analyzes how privacy-preserving the current design is and what the main privacy concerns are (see research question 2). A privacy impact assessment has been conducted to systematically analyze the privacy impact of the ISO/IEC 15118 charging protocol. The assessment concluded that several privacy concerns exist, such as the use of personally identifiable information as well as indirect private information leakage.

The privacy impact assessment lead to consider privacy-preserving alternatives for the privacy invasive steps of the ISO/IEC 15118 protocol. By applying step-by-step modifications to the ISO/IEC 15118 protocol, removing the privacy concerns one after another, the privacy-preserving POPCORN protocol was developed (see research question 3). To complete the POPCORN protocol design, the concrete technologies used to offer the privacy protection were discussed, such as anonymous credentials and group signatures.

Finally, the privacy impact of the POPCORN protocol was evaluated using the privacy impact assessment (see research question 4). The assessment concluded that the POPCORN protocol considered all suggestions offered by the ISO/IEC 15118 privacy assessment and gives final remarks on credential storage and issuance. The POPCORN protocol offers a completely privacy-preserving charging solution by design. To test the practicality of the POPCORN protocol and to easily demonstrate the protocol, a proof-of-concept has been implemented. Abuse scenario were also tested with the implementation, to understand how the protocol will react. All disputes could be solved and the resulting suggestions have been applied to the POPCORN protocol to offer better accountability during dispute resolution.

The POPCORN protocol has shown that it is possible to design and build a technical privacy-preserving charging system that uses contract-based billing. The modular design of the POPCORN protocol allows parts of the protocol to be replaced with non-technical privacy protection mechanisms to reduce the need for additional infrastructure, or to build less privacy-preserving charging solutions with less effort. Nevertheless, a full implementation of the POPCORN protocol offers the best privacy protection.

The POPCORN infrastructure allows additional use-cases, such as authentication and payment of

third party services using the mobility contract. Future work can identify such use-cases in more detail. Further, as part of future work, the POPCORN protocol should be implemented on actual electric vehicle and charging station hardware to analyze the speed concerns encountered during the proof-of-concept implementation. The overhead compared to a normal ISO/IEC 15118 implementation should be examined and whether this effects the overall charging session. Finally, the scalability of the protocol has to be evaluated.

Bibliography

[1] ABC4Trust. ABC4Trust – Attribute-based Credentials for Trust. https://abc4trust.eu/, 2012.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic databases. In *Proceedings of the 28th international conference on Very Large Data Bases*, VLDB '02, pages 143–154. VLDB Endowment, 2002.

[3] G. Alpár (Radboud University). Collis: Anonymous credentials. http://www.cs.ru.nl/~gergely/objects/Collis_AnonCreds_24-11-2011.ppt (slides), Nov 2011.

[4] I. Armac, A. Panchenko, M. Pettau, and D. Retkowitz. Privacy-friendly smart environments. In *Next Generation Mobile Applications, Services and Technologies, 2009. NGMAST '09. Third International Conference on*, pages 425 –431, sept. 2009.

[5] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In M. Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 255–270. Springer Berlin Heidelberg, 2000.

[6] D. Beerda. Electric driving in the netherlands, policy recommendations for dutch national and local authorities to stimulate electric driving in the netherlands. *IVEM Publicaties - Rijksuniversiteit Groningen - Master Thesis*, 2009.

[7] M. Bellis. History of electric vehicles. http://inventors.about.com/od/estartinventions/a/History-Of-Electric-Vehicles.htm (Accessed Aug. 2012), 2012.

[8] P. Bichsel, J. Camenisch, T. Groß, and V. Shoup. Anonymous credentials on a standard java card. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 600–610, New York, NY, USA, 2009. ACM.

[9] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology—CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Berlin: Springer-Verlag, 2004.

[10] A.-M. Borbely and J. F. Krieder. *Distributed Generation – The Power Paradigm for the New Millennium*. CRC Press, 2001.

[11] Bosch Software Innovations GmbH . eMobility White Paper: The Core Processes for Emerging Business Models. http://www.bosch-si.com/white-paper-emobility-core-processes.html, 2011.

[12] Bosch Software Innovations GmbH . EV Charging Infrastructure – eMobility Solution. http://www.bosch-si.com/fileadmin/pdf-en/brochure/201108eMobility_Solution_en.pdf, 2011.

[13] Bosch Software Innovations GmbH . Factsheet: eMobility software solutions - Paving the way for successful mobility concepts. http://www.bosch-si.com/fileadmin/pdf-en/press/FactSheet_eMobilitySolutions1_EN.pdf, 2011.

[14] G. Brauner. Infrastructure for electrical mobility [Infrastrukturen der Elektromobilität]. *Elektrotechnik und Informationstechnik*, 125(11):382–386, 2008.

[15] A. Brooks (AC Propulsion, Inc.). Electric drive vehicles: A huge new distributed energy resource (slides), vehicle-to-grid session at the electric transportation industry conference, sacramento, calif. http://www.lifepo4.info/Battery_study/Presentation/A_Brooks_ETI_conf.pdf (Accessed Aug. 2012), 2001.

[16] Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit. Nationale Plattform Elektromobilität. http://www.bmu.de/verkehr/elektromobilitaet/nationale_plattform_elektromobilitaet/doc/45970.php, 2010.

[17] J. Camenisch and T. Groß. Efficient attributes for anonymous credentials. *ACM Trans. Inf. Syst. Secur.*, 15(1):4:1–4:30, Mar. 2012.

[18] J. Camenisch and J. Groth. Group signatures: Better efficiency and new theoretical aspects. In *Proceedings of the 4th international conference on Security in Communication Networks*, SCN'04, pages 120–133, Berlin, Heidelberg, 2005. Springer-Verlag.

[19] J. Camenisch, M. Kohlweiss, and C. Soriente. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC '09*, Irvine, pages 481–500, Berlin, Heidelberg, 2009. Springer-Verlag.

[20] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '01, pages 93–118, London, UK, UK, 2001. Springer-Verlag.

[21] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In M. Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72. Springer Berlin Heidelberg, 2004.

[22] J. Camenisch and E. Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, pages 21–30, New York, NY, USA, 2002. ACM.

[23] J. Camenisch (IBM Zurich). 2nd European Trusted Infrastructure Summer School: Group Signatures. http://summerschool.trust.ruhr-uni-bochum.de/papers/Jan-Camenisch-2007.pdf (slides), Oct 2007.

[24] A. Cavoukian. Privacy by design: Best practices for privacy and the smart grid. In N. Pohlmann, H. Reimer, and W. Schneider, editors, *ISSE 2010 Securing Electronic Business Processes*, pages 260–270. Vieweg+Teubner, 2011. 10.1007/978-3-8348-9788-6_25.

[25] A. Cavoukian, J. Polonetsky, and C. Wolf. Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*, 3:275–294, 2010. 10.1007/s12394-010-0046-y.

[26] CEN, CENELEC, Focus Group on European Electro-Mobility. Standardization for road vehicles and associated infrastructure – Report in response to Commission Mandate M/468 concerning the charging of electric vehicles. ftp://ftp.cen.eu/CEN/Sectors/List/Transport/Automobile/EV_Report_incl_annexes.pdf, 2011.

[27] D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, pages 199–203, 1982.

[28] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO' 88*, volume 403 of *Lecture Notes in Computer Science*, pages 319–327. Springer Berlin / Heidelberg, 1990. 10.1007/0-387-34799-2_25.

[29] D. Chaum and E. Heyst. Group signatures. In D. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer Berlin Heidelberg, 1991.

[30] R. Clarke. Privacy impact assessments. http://www.rogerclarke.com/DV/PIA.html (Accessed Aug. 2012), 2003.

[31] M. Crotti, D. Ferri, F. Gringoli, M. Peli, and L. Salgarelli. PP2db: A Privacy-Preserving, P2P-Based Scalable Storage System for Mobile Networks. In M. Rajarajan, F. Piper, H. Wang, and G. Kesidis, editors, *Security and Privacy in Communication Networks*, volume 96 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 533–542. Springer Berlin Heidelberg, 2012.

[32] C. Cuijpers and B.-J. U. v. T. Koops. Het wetsvoorstel 'slimme meters': Een privacytoets op basis van art. 8 EVRM (Onderzoek in opdracht van de Consumentenbond). http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf (Accessed Aug. 2012), 2008.

[33] A. A. Cárdenas and R. Safavi-Naini. Chapter 25 - security and privacy in the smart grid. In *Handbook on Securing Cyber-Physical Critical Infrastructure*, pages 637 – 654. Morgan Kaufmann, Boston, 2012.

[34] N. Desmoulins, S. Canard, and J. Traoré (Orange Labs R&D, France). 3rd International Conference on Trust and Trustworthy Computing: Java Implementation of Group and Blind Signatures. http://www.trust2010.org/slides/Desmoulins.pdf (slides), Jun 2010.

[35] Deutsches Institut für Normung. DIN SPEC 91286:2011-11: Electric mobility – Schemes of identifiers for E-Roaming – Contract ID and Electric Vehicle Supply Equipment ID. discussed in http://www.lebenswelt-elektromobilitaet.de/media/Pr\unhbox\voidb@x\bgroup\accent127a\penalty\@M\hskip\z@skip\egroupsentationen/20110910_VorstellungDINSPEC91286_Mannheim.pdf, Nov 2011. http://www.beuth.de/en/technical-rule/din-spec-91286/145915787.

[36] C. T. Di Iorio, F. Carinci, J. Azzopardi, V. Baglioni, P. Beck, S. Cunningham, A. Evripidou, G. Leese, K. F. Lovaas, G. Olympios, M. Orsini Federici, S. Pruna, P. Palladino, S. Skeie, P. Taverner, V. Traynor, and M. Massi Benedetti. Privacy impact assessment in the design of transnational public health information systems: The biro project. *Journal of Medical Ethics*, 35(12):753–761, 2009.

[37] I. Diefenbach (RWE E-Mobility). 7. CIGRE/CIRED-Informationsveranstaltung: Elektromobilität aus Sicht der Energieversorgungsunternehmen. http://webconferencing2.dke.de/de/Verband/Partnerorganisationen/DK-CIGRE/Veranstaltungen/Documents/Vortrag_Diefenbach.pdf (slides), 2009.

[38] DLMS User Association. What is DLMS/COSEM. http://www.dlms.com/information/whatisdlmscosem/index.html and http://www.dlms.com/downloads/we-speak-the-same-language.pdf (Accessed Aug. 2012), 2011.

[39] Economist – Technology Quarterly. Building the smart grid. Print Edition and at http://www.economist.com/node/13725843 (Accessed Aug. 2012), 2009.

[40] A. Enache. About group digital signatures. *Journal of Mobile, Embedded and Distributed Systems*, 4(3), 2012.

[41] Energy Future Coalition. Challenge and opportunity: Charting a new energy future. http://energyfuturecoalition.org/files/webfmuploads/EFC_Report/EFCReport.pdf (Accessed Aug. 2012), 2003.

[42] escrypt GmbH/Inc. Security meets electric mobility – With the project SecMobil® toward worldwide Leadership in the field of IT security for electric mobility . https://www.escrypt.com/fileadmin/escrypt/pdf/Press_release_long_SecMobil.pdf, 2012.

[43] EURELECTRIC Task Force Electric Vehicles. Facilitating e-mobility: EURELECTRIC views on charging infrastructure. http://www.eurelectric.org/media/27060/0322_facilitating_emobility_eurelectric_views_-_final-2012-030-0291-01-e.pdf, 2012.

[44] European Parliament and the Council of 12 July 2002. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT, July 2002.

[45] European Parliament and the Council of 24 October 1995. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT, October 1995.

[46] R. Falk and S. Fries. Securing the electric vehicle charging infrastructure - current status and potential next steps. In *27. VDI/VW-Gemeinschaftstagung*, volume VDI-Berichte 2131 (ISBN 978-3-18-092131-0), pages p. 3–15. VDI Wissensforum GmbH, 2011.

[47] R. Falk and S. Fries. Smart grid cyber security - an overview of selected scenarios and their security implications. *Praxis der Informationsverarbeitung und Kommunikation*, 34(4):168–175, 2011.

[48] H. Fhom and K. Bayarou. Towards a holistic privacy engineering approach for smart grid systems. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pages 234 –241, nov. 2011.

[49] FiA (Fédération Internationale de l'Automobile). Towards E-Mobility - The challenges ahead. http://www.lowcvp.org.uk/assets/reports/emobility_full_text_fia.pdf, 2011.

[50] J. Fluhr (FIR e. V. RWTH Aachen). Symposium Lebenswelt Elektromobilität:DIN SPEC 91286. http://www.lebenswelt-elektromobilitaet.de/media/Pr\unhbox\voidb@x\bgroup\accent127a\penalty\@M\hskip\z@skip\egroupsentationen/20110910_VorstellungDINSPEC91286_Mannheim.pdf (slides), Sep 2011.

[51] A. Foley, I. Winning, and B. Gallachóir. State-of-the-art in electric vehicle charging infrastructure. In *Vehicle Power and Propulsion Conference (VPPC), 2010 IEEE*, pages 1 –6, sept. 2010.

[52] Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO & PricewaterhouseCoopers AG. Elektromobilität – Herausforderungen für Industrie und öffentliche Hand. www.iao.fraunhofer.de/images/downloads/elektromobilitaet.pdf, 2010.

[53] M. Hable, C. Schwaegerl, L. Tao, A. Ettinger, R. Köberle, and E.-P. Meyer. Requirements on electrical power infrastructure by electric vehicles. In *Emobility - Electrical Power Train, 2010*, pages 1 –6, nov. 2010.

[54] R. Hinden and S. Deering. IP Version 6 Addressing Architecture. RFC 4291 (Draft Standard), Feb 2006. Updated by RFCs 5952, 6052.

[55] R. Housley, W. Polk, W. Ford, and D. Solo. RFC 3280 - Internet X.509 Public Key Infrastructure Certificate. Technical report, IETF, 2002.

[56] IBM Research Zurich. Usage of Identity Mixer. http://www.zurich.ibm.com/idemix/usage.html, 2012.

[57] IBM Research Zurich, PrimeLife, and PRIME. Identity Mixer – Download. https://prime.inf.tu-dresden.de/idemix/, 2012.

[58] Information & Privacy Commissioner, Ontario, Canada. Privacy by design. http://privacybydesign.ca/.

[59] Information Commissioner's Office. Privacy impact assessment (PIA). http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx (Accessed Aug. 2012), 2012.

[60] ISO. Road vehicles – Vehicle-to-Grid Communication Interface – Part 1: General information and use-case definition (Draft). 2012.

[61] ISO. Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements (Draft). 2012.

[62] A. Kovacs (BroadBit). PowerUp - Vehicle2Grid Technology for Fully Electric Vehicles (Introdution presentation slides). http://www.powerup.org, 2011.

[63] A. Kung, J.-C. Freytag, and F. Kargl. Privacy-by-design in its applications - the way forward. In *Second International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN 2011)*, Lucca, Italy, 06/2011 2011.

[64] J. Lapon, M. Kohlweiss, B. De Decker, and V. Naessens. Analysis of revocation strategies for anonymous idemix credentials. In *Proceedings of the 12th IFIP TC 6/TC 11 international conference on Communications and multimedia security*, CMS'11, pages 3–17, Berlin, Heidelberg, 2011. Springer-Verlag.

[65] A. S. Massoud and B. Wollenberg. Toward a smart grid: Power delivery for the 21st century. *Power and Energy Magazine, IEEE*, 3(5):34 – 41, sept.-oct. 2005.

[66] G. Medvinsky and C. Neuman. Netcash: A design for practical electronic currency on the internet. In *Proceedings of the 1st ACM conference on Computer and communications security*, CCS '93, pages 102–106, New York, NY, USA, 1993. ACM.

[67] Microsoft Research and ABC4Trust. U-Prove. http://research.microsoft.com/en-us/projects/u-prove/, 2012.

[68] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys 2010)*, Zurich, Switzerland, Nov. 2010.

[69] T. Narten, R. Draves, and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941 (Draft Standard), Sept. 2007.

[70] G. Neven (IBM Zurich). NIST Meeting on Privacy-Enhancing Cryptography: IBM Identity Mixer (idemix). http://csrc.nist.gov/groups/ST/PEC2011/presentations2011/neven.pdf (slides), Dec 2011.

[71] H. Nissenbaum. Privacy as Contextual Integrity. *Washington Law Review*, 79(1):119–158, Feb. 2004.

[72] Oracle Corporation. OpenJDK. http://openjdk.java.net/, 2012.

[73] Organisation for Economic Co-operation and Development (OECD). OECD Privacy Principles. http://oecdprivacy.org, 2010.

[74] C. Paar, A. Rupp, A. Weimerskirch, and W. Burleson. Securing green cars: IT security in next-generation electric vehicle systems. In *Proceedings of the Annual Meeting and Exposition of the Intelligent Transportation Society of America*, 2009.

[75] PBS. Timeline: History of the electric car. http://www.pbs.org/now/shows/223/electric-car-timeline.html (Accessed Aug. 2012), 2009.

[76] R. A. Popa, H. Balakrishnan, and A. J. Blumberg. VPriv: Protecting privacy in location-based vehicular services. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, pages 335–350, Berkeley, CA, USA, 2009. USENIX Association.

[77] PrimeLife Project. PrimeLife - bringing sustainable privacy and identity management to future networks and services. http://primelife.ercim.eu/, Oct 2011.

[78] Raspberry Pi Foundation. Raspberry Pi - An ARM GNU/Linux box. http://www.raspberrypi.org/, 2012.

[79] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM Trans. Inf. Syst. Secur.*, 1(1):66–92, Nov. 1998.

[80] A. Rial and G. Danezis. Privacy-preserving smart metering. In *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, WPES '11, pages 49–60, New York, NY, USA, 2011. ACM.

[81] Russell McVeagh McKenzie Bartleet & Co. *Intellectual Property and Media Law Update: The Privacy Act 1993 : The Honeymoon is Over*. Russell McVeagh McKenzie Bartleet & Company, 1996.

[82] RWE Effizienz GmbH. RWE eMobility. www.rwe-mobility.com, 2012.

[83] S. Ashley (SAE International). A new drive toward wireless EV charging. http://www.sae.org/mags/sve/ENRG/11035 (Accessed Aug. 2012), 2012.

[84] G. Sammer, D. Meth, and C. J. Gruber. Elektromobilität – die sicht der nutzer. *e & i Elektrotechnik und Informationstechnik*, 125:393–400, 2008.

[85] J. Schmutzler, S. Groning, and C. Wietfeld. Management of distributed energy resources in iec 61850 using web services on devices. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 315 –320, oct. 2011.

[86] M. Schneider, S. Tcaciuc, and C. Ruland. Secure metering for electrical vehicles. In *Emobility - Electrical Power Train, 2010*, pages 1 –6, nov. 2010.

[87] B. Schneier. Why 'anonymous' data sometimes isn't. http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213 (Accessed Aug 2012), Dec 2007.

[88] Security Team, IBM Research Zurich. Specification of the Identity Mixer Cryptographic Library. IBM Research Report 3730, IBM Research, Apr 2010.

[89] W. Smit and E. van Oost. *De wederzijdse beinvloeding van technologie en maatschappij: Een Technology Assessment-benadering*. Coutinho, 1999.

[90] D. Solove. *Understanding privacy*. Number v. 10 in Understanding privacy. Harvard University Press, 2008.

[91] D. J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):p477+, Jan. 2006.

[92] G. Spiegelberg (Siemens AG). The eCar in its smart grid infrastructure - an holistic approach of Siemens AG. http://www.vt.bv.tum.de/uploads/verkehraktuell/Verkehr%20aktuell_web%_Prof.%20Spiegelberg_10-10-28.pdf (slides), 2010.

[93] B. Stewart. Privacy impact assessments. *Privacy Law and Policy Reporter*, (3):61–64, 1996.

[94] C. Sulzberger. An early road warrior: electric vehicles in the early years of the automobile. *Power and Energy Magazine, IEEE*, 2(3):66 – 71, may-june 2004.

[95] Tor Project. Anonymity online. https://www.torproject.org/, 2012.

[96] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel. PriPAYD: Privacy friendly pay-as-you-drive insurance (journal version). *IEEE Transactions on Dependable and Secure Computing*, page 14, 2010.

[97] I. T. Union. ITU-T Recommendation X.509 — ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks". Technical report.

[98] United States Government CIO Council. Best practices: Privacy – internal revenue service model information technology PIA. www.cio.gov/Documents/pia_for_it_irs_model.pdf (Accessed Aug. 2012), 2000.

[99] United States Government Department of Homeland Security. Privacy office - privacy impact assessments (PIA). http://www.dhs.gov/privacy-office-privacy-impact-assessments-pia (Accessed Aug. 2012), 2012.

[100] Università degli Studi di Brescia. PP2db: A Privacy-Preserving, P2P-based Scalable Storage System for Mobile Networks. http://www.ing.unibs.it/ntw/tools/pp2db/, 2011.

[101] K. Verslype, P. Verhaeghe, J. Lapon, V. Naessens, and B. Decker. Priman : A privacy-preserving identity framework. In S. Foresti and S. Jajodia, editors, *Data and Applications Security and Privacy XXIV*, volume 6166 of *Lecture Notes in Computer Science*, pages 327–334. Springer Berlin Heidelberg, 2010.

[102] Volkswagen AG. Global Automakers to Demo EV Fast Charging at EVS26. http://www.volkswagenag.com/content/vwcorp/info_center/en/news/2012/05/global_automakers_to_demo_ev_fast_charging_at_evs26.html, 2012.

[103] S. Walther, I. Markovic, A. Schuller, and A. Weidlich. Classification of business models in the e-mobility domain. In *Proceedings of the 2nd European Conference Smart Grids and EMobility*, number i, pages 35–42, 2010.

[104] S. Warren and L. Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193, 1890.

[105] A. F. Westin. *Privacy and Freedom*. The Bodley Head Ltd, 1967.

[106] Wirtschaftsministerium Baden-Württemberg, e-mobil BW GmbH, Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO). Systemanalyse BWe mobil – IKT- und Energieinfrastruktur für innovative Mobilitätslösungen in Baden-Württemberg. http://www.e-mobilbw.de, 2010.

[107] D. Wright and P. de Hert. *Privacy Impact Assessment*. Springer, 2011.

[108] Z. Yang, S. Yu, W. Lou, and C. Liu. P2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid. *IEEE Trans. Smart Grid*, 2(4):697–706, 2011.