POPCORN: Privacy-Preserving Charging for eMobility

MSc **Christina Höfer**, Dr. **Jonathan Petit**, University of Twente, Enschede, The Netherlands;
Dr.-Ing. **Robert Schmidt**, DENSO Automotive Dtld. GmbH, Eching;
Prof. Dr. rer. nat. **Frank Kargl**, Universität Ulm & University of Twente;

Abstract

Upcoming years will see a massive deployment of electric vehicles and hence charging infrastructure. This will require protocols and standards that control authentication, authorization, and billing of electric vehicle charging. The ISO/IEC 15118 protocol addresses the communication between the charging station and the electric vehicle and will likely play an important role in Europe. While it foresees security protection, there are no significant mechanisms for privacy protection in place. In this paper, we investigate the privacy protection of ISO/IEC 15118 by means of a Privacy Impact Assessment (PIA). Based on this we propose modular extensions to the protocol using state-of-the-art Privacy Enhancing Technologies (PETs) like anonymous credentials to create a system with maximum privacy protection.

1. Introduction

Mobility in the future has to become more eco-friendly. Especially, in urban scenarios the move towards electric mobility is already becoming visible. This will significantly change our transportation systems work, especially as electric vehicles will recharge more often compared to the refueling of traditional cars. Charging of *Electric Vehicles* (EVs) is a central aspect of the electric vehicle introduction. Ideally, for the driver charging an EV will be as simple as parking – just park, plugin, and charging begins. Still, for charging control, authorization, and billing purposes, a lot of information has to be exchanged automatically between the EV and the *Electric Vehicle Supply Equipment* (EVSE), also known as *Charging Station/Spot* (CS). Especially the multitude of different vehicle types and their electrical characteristics and requirements require a thorough setup of the EVSE. In addition, frequent charging will also require frequent payments. The payment should be done without user-interaction for maximum convenience. The standard ISO/IEC 15118-1 [6] therefore defines actors and protocols to perform load management, billing and clearing, as well as certification.

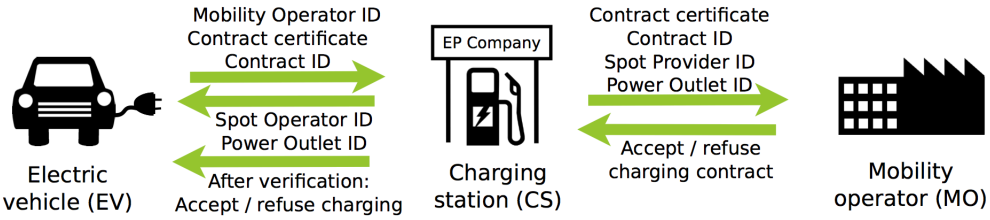

Figure 1: ISO/IEC 15118 contract authentication

ISO/IEC 15118 defines a number of different payment options. In case of the most user-friendly charging management, a contract with a so-called *Mobility Operator* (MO) has to be concluded in advance. In its simplest form, the MO can be the utility provider of the user that will collect charging fees together with the monthly energy bill. However, the MO can also be a separate entity that charges the fees to the user's account. Signing up with an MO involves issuing of cryptographic X.509 certificates to vehicles or drivers. For charging authentication the EV sends its identifiers to the CS, which in turn asks the MO for confirmation (see Fig. 1). During the charging loop, the EV has to periodically provide digital signatures for the cumulative meter readings provided by the CS. After each charging session the MO receives a *Service Detail Record* (SDR) from the charging station containing the information required to pay the *Energy Provider* (EP) that operates the CS. The charging spot also informs its energy provider about each charging session by sending the EV-signed meter receipts. The energy provider can use the receipts in case of disputes. At the end of a certain period, say one month, the MO provides a bill to the contracted user for the received SDRs. If the MO is also the utility provider of the user, the bill for EV charging will be added to the user's domestic energy bill. The charging and payment communication is illustrated in Fig. 2.

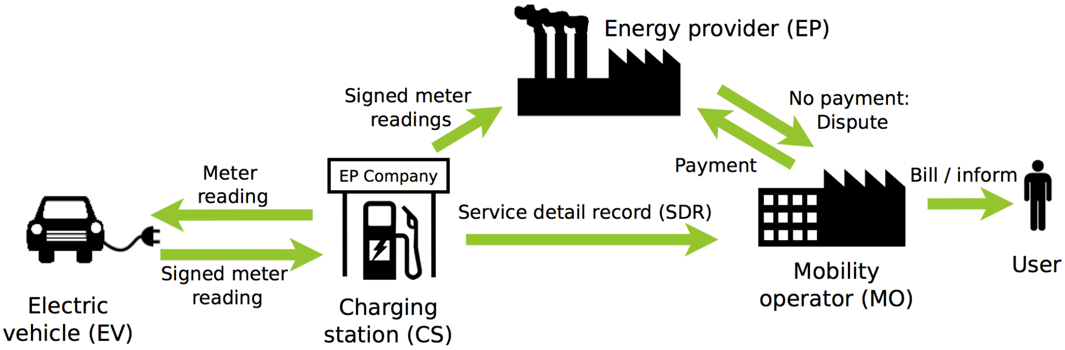

Figure 2: ISO/IEC 15118 charging and payment communication

To allow flexible charging while traveling, we assume that the MO has roaming agreements with a variety of different EPs similar to roaming agreements between cellphone operators.

Assuming that many different EPs will be active in the market, roaming may become the norm rather than the exception.

ISO/IEC 15118 already defines detailed communication protocols and the corresponding application- layer messages in ISO/IEC 15118-2 [7] including security mechanisms based on TLS and XML Security. While these security measures may be appropriate to ensure security, the standard does not explicitly address privacy. ISO/IEC 15118 actually raises privacy as a concern, but there are no specific measures taken for privacy protection. In this paper we present a detailed privacy analysis of ISO/IEC 15118 and propose modular privacy enhancements that lead to a fully privacy-preserving charging protocol for electric vehicles.

2. Privacy Problems

At the first glance, ISO/IEC 15118 protocol possible privacy issues. As can be seen from Figure 1 and 2, the EV and the charging stations exchange a lot of potentially personally identifiable information (PII). This leads to scenarios where a charging station and energy provider may learn the home location of a vehicle, esp. if the vehicle is registered with a small mobility operator that operates, e.g., only within a city. Beyond, the vehicle uses a specific certificate to authenticate. As a result, the vehicle may be tracked and its home location identified wherever it travels. Likewise, the mobility operator learns the IDs of all charging spots where its customers charge. While anonymous payment alternatives exist, we expect that the convenience to simply drive to a charging station, plug-in the electricity cable, and then find the charge added to the home utility's electricity bill will make many drivers choose this option. This motivated us to investigate the privacy aspects of electric vehicle charging and design a fully privacy-friendly solution.

As a first step, we have conducted a Privacy Impact Assessment (PIA) [11] of the current standard draft with the contract-based payment option. Our PIA approach includes the following steps: 1. *Scope and purpose definition*, 2. *Stakeholders*, 3. *Information assets*, 4. *Information requirements and use*, 5. *Information handling and other considerations*, 6. *Evaluation*. Due to space constraint we only summarize the findings of the first three steps and then present the results. Consider [4] for the complete PIA.

(1) Scope and purpose definition

This PIA analyzes the ISO/IEC 15118, in particular the contract-based payment scenario, from the point of view of the user, i.e., the driver or owner of the EV. The purpose of the assessment is to systematically identify the privacy risks of ISO/IEC 15118. Further, we hope to identify areas of the protocol where less privacy-invasive approaches or privacy-preserving alternatives can be used.

(2) Stakeholders

The following stakeholders are involved in the charging infrastructure:

Electric vehicle (EV) user: This is the legal entity using the vehicle, i.e., the EV owner and in most cases the driver of the EV. The user has signed a mobility contract with the MO.

Charging station (CS): The CS is the EV's communication partner in terms of the protocol. The CS communicates with the vehicle to negotiate the charging parameters, manage power delivery and to handle the payment.

CS's energy provider (EP): The EP operates the CS and receives the payment for the electricity. For accountability, we assume that the EP wants to link the energy consumption to a payment and has access to the data recorded by the charging station unless otherwise specified in the standard.

EV's mobility operator (MO): The MO has a charging contract with the EV user. The mobility operator may be the same energy provider as the one operating the CS, a different one or a third party. For the PIA we assume that the MO is different from the charging station's EP (EV is roaming) and that the MO is the user's home domestic supplier.

(3) Information assets

To determine the information assets, the use case descriptions [6] and messages of the ISO/IEC 15118 protocol [7] are examined to find out what information exists in the system, where it comes from and with whom it is shared. Information assets can come in different forms, such as identifiers, certificates, and signatures. Privacy risks are caused by information that uniquely identify the EV (and hence its user) and information that indirectly reveals information about the vehicle.

After analyzing the information assets it can be concluded that the following certificates and identifiers are personally identifiable information: Contract ID and contract certificate, identity certificate and any attribute certificate linked it, customer ID, EV ID and MAC address, the signed meter readings, and the service detail records. In addition, the following information assets may reveal privacy sensitive information when linked with a personally identifiable information asset: Mobility operator ID, EVSE ID and Power outlet ID, EVSE operator ID (the EP), and timestamps.

PIA evaluation

The PIA identified the following privacy invasions (PI):

PI 1. *Excessive use of PII (e.g., contract ID):* The contract ID that uniquely identifies the electric vehicle and/or the driver is used in almost all phases of the communication, starting even at service discovery and is made available both to the CS, the EP, and the MO. We have identified that most of these protocol steps do not necessarily mandate revealing the contract ID as long as there are no disputes over the payment. Further identifiers exist that uniquely identify the EV, such as the Provisioning Certificate and Cert ID, the Identity Certificate and the Customer ID. Overall, the protocol uses multiple PII in different protocol steps, which jeopardizes the privacy.

PI 2. *Revealing the MO in conjunction with an EV-identifier:* The CS can deduce the MO by considering the Contract ID, which contains the MO identifier [3]. In case the MO is a small local energy supplier, the ID may reveal in which city or area the EV user lives.

PI 3. *Revealing the CS in conjunction with an EV-identifier:* During contract validation the charging station includes its own identifiers (Spot Operator and Power Outlet ID) when communicating with the backend. The MO will be able to link the EV and the CS, thus learning the exact location and time of the charging effectively allowing tracking of the vehicle. This is especially true for the MO who will receive all SDRs that a vehicle creates. The MO will have a complete record of the places where its customers charge.

PI 4. *Revealing the EP in conjunction with an EV-identifier:* Analogue to the above case with the MO, if the EP is a small local energy provider, this will also reveal the rough location of a vehicle to recipients, esp. to the MO.

So even 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” [6], the privacy impact assessment has shown that significant privacy risks exist. The PIA recommends minimizing the use of PII and to replace necessary information by privacy-preserving alternatives. Further, the information flow should be altered to avoid disclosing sensitive information to parties that do not require the information.

In the remainder of this paper, we will use a multi-step approach to design a privacy-enhanced version of the ISO/IEC 15118 protocol called *POPCORN*. Using the POPCORN protocol, none of the eMobility stakeholders, e.g., the charging station, energy provider, or mobility operator, can track an EV, and hence the user, or obtain other private information during a charging process. This is our privacy requirement. In addition, the protocol takes into account the privacy principles as summarized by the Organization for Economic Cooperation and Development (OECD) [8]. In particular, the “Collection Limitation”, and the “Use Limitation” principle are used as protocol requirements.

3. Enhancing Privacy Protection

The POPCORN protocol is developed as step-wise modifications of the ISO/IEC 15118 protocol, based on the findings of the PIA. The step-by-step privacy enhancements ensure that all privacy concerns are systematically removed from ISO/IEC 15118, while preserving the functionality.

POPCORN
Privacy-Preserving ChaRgiNg
for e-mobility

3.1 The ISO/IEC 15118 enhancement steps

The ISO/IEC 15118 protocol is modified in four steps to obtain the POPCORN protocol.

Step 1: Minimizing PII The first step reduces the use of personally identifiable information to the minimum. Unused unique vehicle identifiers, such as the Customer ID, do not need to be sent to the charging station. Furthermore, the charging station can perform contract authentication locally without communicating information to the backend. ISO/IEC 15118 requires that each charging station has the root certificates installed. This eliminates the need for privacy-sensitive contract authentication with the backend.

Step 2: Privacy-preserving functional alternatives The second enhancement is to replace privacy-sensitive ISO/IEC 15118 procedures with privacy-preserving ones.

Contract authentication: The uniquely identifying Contract ID and Certificate that is used by ISO/IEC 15118 for charging authentication are replaced with *anonymous credentials* in the POPCORN protocol. Anonymous credentials allow selective disclosure of credential attributes, while hiding other attributes. In addition, anonymous credentials can be used to disclose properties of credential attributes without revealing the actual value. As concrete implementation for the POPCORN protocol, the Idemix anonymous credential system [2, 5] has been chosen. The Idemix anonymous credentials offer multi-show unlinkability and attribute property proofs. The charging contract details, including the expiration date and tariff information, are stored in an anonymous credential. For authentication, the vehicle proofs that its contract is valid based on an equality proof over the expiration date and the current date. Similarly, special tariffs and conditions can be communicated to the charging station without revealing the vehicle's identity. The charging station can locally verify the contract proof, so that offline charging is also possible. The anonymous credentials can be set to have a short lifetime independent of the expiration date of the contract, so that no other revocation strategies are required. When the lifetime has expired, the vehicle downloads a credential update and applies it to the expired credential to reactivate it. ISO/IEC 15118 already defines messages for certificate updates. One of the described methods provides a communication link to the issuer of the credentials. This approach can be used, so that no additional update methods are required. If this is to happen online before charging, it is required that this communication link does not reveal the location of the vehicle.

Meter receipts: ISO/IEC 15118 requires the electric vehicle to sign the meter readings during the charging loop to offer non-repudiation. These commits directly reveal the identity of the vehicle. For the POPCORN protocol, the charging commits are created using *group signatures*. Short group signatures [1] offer a suitable implementation for the POPCORN protocol.

Using group signatures the identity of the signing electric vehicle remains hidden from the charging station and the energy provider, while the signatures are verifiable by all parties. The created signatures of all vehicles are indistinguishable from each other; only the group manager can reveal the identity of the vehicle. The POPCORN protocol adds a trusted dispute resolver (DR) to the charging infrastructure to fulfill the group manager role. In case of disputes, e.g., if a charging bill has not been paid, the dispute resolver can be contacted to verify and solve the dispute. The dispute resolver will uncover the vehicle's identity and contact the responsible mobility operator to resolve the dispute. The energy provider will not be informed about the vehicle's identity. At contract establishment, each electric vehicle obtains its group signing credentials.

Step 3: Privacy-preserving information flow The third enhancement makes the information flow privacy-preserving, breaking up the direct interaction between the CS/EP and the MO. This is achieved by either redirecting the messages via non-privacy-sensitive routes or by using privacy-preserving communication means, e.g., via privacy-proxies and TOR networks [10]. For example, one option is to send the service detail record from the vehicle to the mobility operator rather than via the charging station to the mobility operator.

Step 4: Privacy-preserving payment The final enhancement aims to make the payment privacy-preserving. A trusted payment handler (PH) is added to the charging infrastructure to forward the payment from the mobility operator to the receiving energy provider. After charging, the charging station sends the partial SDR to the electric vehicle and the energy provider. The EV appends its Contract ID to the SDR and submits it to the mobility operator. The MO has all the information to bill the user and to pay the energy provider. The recipient details are encrypted in the SDR and remain unknown to the payee; only the payment handler can decrypt the information. A random transaction number given in the SDR is used to link the payment to the specific charging session, so that the receiver can verify whether the payment is correct. In addition to this enhancement step, the format of the service detail record has been redefined as specified in Table 1.

Table 1: Content of the SDR for the POPCORN protocol.

Field	**Special properties**
Amount of electricity consumed & tariff	—
Amount payable	—
Recipient of the payment (EP)	Encrypted for payment handler
Session/transaction number	—
Contract ID	Appended by vehicle, encrypted for MO
EV signature over complete SDR	Appended by vehicle, encrypted for MO

3.2 The POPCORN protocol

The final POPCORN steps are illustrated in Fig. 3 and 4. Figure 3 describes the contract establishment. These steps are only required when the EV user signs a new mobility contract and has to set up its anonymous credentials and group signature key.

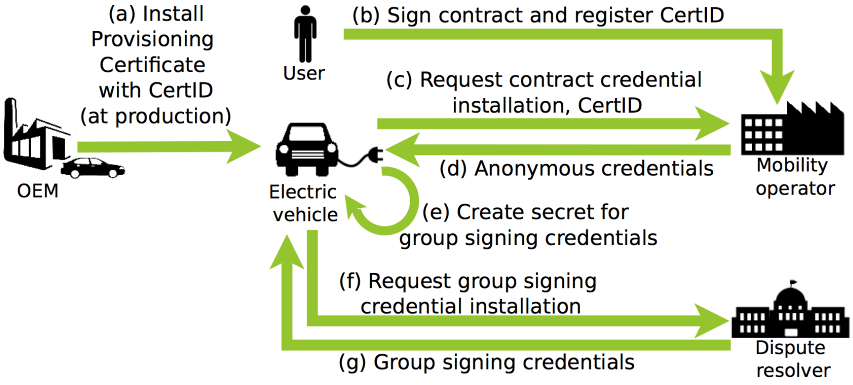
(a) Install Provisioning Certificate with CertID (at production)
User
(b) Sign contract and register CertID
(c) Request contract credential installation, CertID
OEM
Electric vehicle
(d) Anonymous credentials
Mobility operator
(e) Create secret for group signing credentials
(f) Request group signing credential installation
Dispute resolver
(g) Group signing credentials

Figure 3: The POPCORN contract establishment.

The phases 1-4, depicted in Fig. 4, occur during every charging session. Phase 1 is the charging authentication. The actual charging, including the meter reading signing, occurs during phase 2. After the charging, in phase 3, the SDR and the signatures are sent. The payment is completed in phase 4. Phase 5 is only required in case of disputes (see Fig. 4).

4. Evaluation

In this section, we evaluate our privacy-preserving charging protocol (POPCORN) with respect to privacy and feasibility.

4.1 PIA of the POPCORN protocol

The PIA as conducted on the ISO/IEC 15118 protocol (see Section 2) is repeated with the

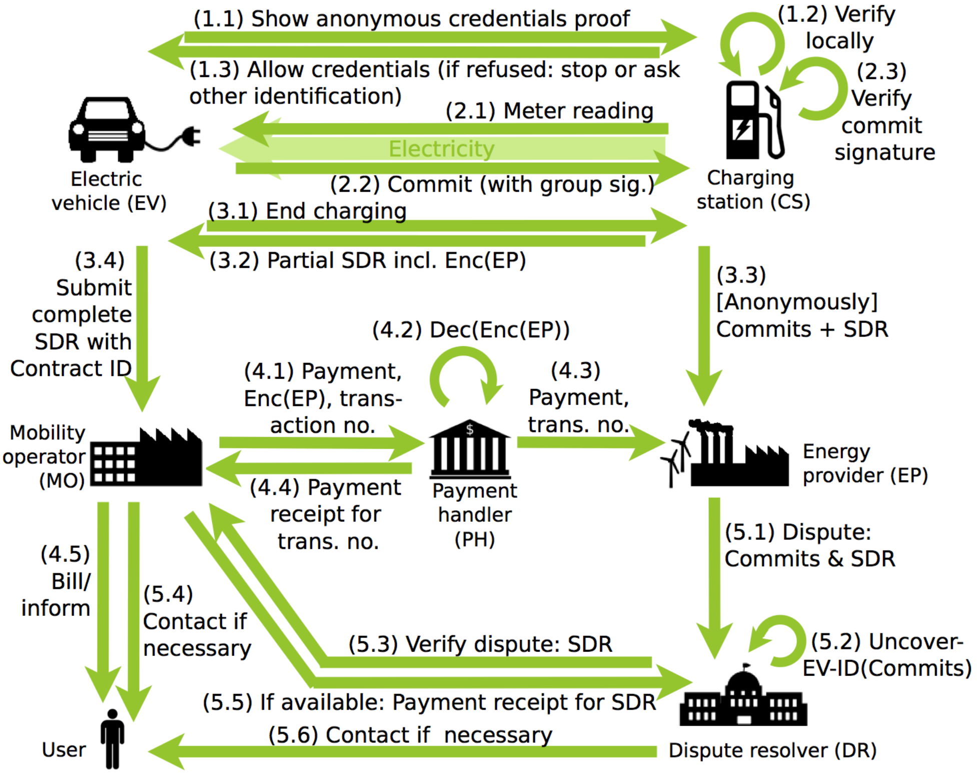
(1.1) Show anonymous credentials proof
(1.2) Verify locally
(1.3) Allow credentials (if refused: stop or ask other identification)
(2.1) Meter reading
Electricity
(2.2) Commit (with group sig.)
(2.3) Verify commit signature
Electric vehicle (EV)
Charging station (CS)
(3.1) End charging
(3.2) Partial SDR incl. Enc(EP)
(3.3) [Anonymously] Commits + SDR
(3.4) Submit complete SDR with Contract ID
(4.1) Payment, Enc(EP), trans-action no.
(4.2) Dec(Enc(EP))
(4.3) Payment, trans. no.
Mobility operator (MO)
Payment handler (PH)
Energy provider (EP)
(4.4) Payment receipt for trans. no.
(4.5) Bill/ inform
(5.4) Contact if necessary
(5.1) Dispute: Commits & SDR
(5.2) Uncover-EV-ID(Commits)
(5.3) Verify dispute: SDR
(5.5) If available: Payment receipt for SDR
(5.6) Contact if necessary
User
Dispute resolver (DR)

Figure 4: The POPCORN protocol for charging with automated billing.

POPCORN protocol to compare the two and identify the added privacy protection that we have reached. We only summarize the findings of the steps (2) and (3) and then present a discussion on the POPCORN protocol. The complete PIA can be found in [4].

(2) Stakeholders

POPCORN introduces two new stakeholders: the *dispute resolver* and the *payment handler*.

Dispute resolver (DR): Being a trusted party, the DR is the group manager for the meter reading signing credentials. The energy provider can contact the DR 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): Handling 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.

(3) Information assets

Next, the messages of the POPCORN protocol are inspected for important information assets. We have identified the following assets as Personally Identifiable Information (PII): Contract ID, anonymous contract credentials, signed meter readings (only towards DR; DR can link EV to EP and MO, but not to a CS), and the service detail record with appended EV data (only towards MO; MO cannot link EV to CS/EP).

Discussion

The goal of the POPCORN protocol is to offer complete privacy-preserving charging by design while using a mobility contract for payment. While there still exist personally identifiable information assets, their use and disclosure has been limited to a required minimum. Using group signatures, the signed meter readings no longer reveal the electric vehicle identity to the charging station or energy provider. Contract verification with the backend is no longer required using privacy-preserving anonymous credentials. In addition, the monetary information flow has been hidden, offering more privacy than the ISO/IEC 15118 PIA suggested.

In summary, all PIA recommendations have been implemented in the POPCORN protocol. The privacy-invasions summarized in Section 2 have been reduced to the minimum. PI2 is avoided altogether. PI1 still occurs when the EV provides its Contract ID together with the SDR to the MO. This cannot be avoided when using a charging contract, as the MO needs to know which EV customer to bill. Dispute resolution results in PI3, since the dispute resolver learns the EV identity together with the MO (PI3) and the EP (PI4). For accountability and non-repudiation 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. It is possible to avoid the PI4, 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 as a denial-of-service attack on the dispute resolver. Further, the payment handler sees the MO-EP payment link, however without any EV identifier involved. 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.

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

4.2 POPCORN proof-of-concept

In order to evaluate the feasibility of POPCORN and to demonstrate the protocol a proof-of-concept, as shown in Figure 5, has been implemented using an electric toy vehicle.

Setup The proof-of-concept is implemented using the Java OpenJDK with each of the six stakeholders being a separate Java process. The hardware setup is depicted in Fig. 5. The electric vehicle and the charging station are each run on a Raspberry Pi computer [9]. This single-board computer was chosen, because it fits in a toy electric car and has GPIO pins that can be used to actually charge the vehicle's batteries. Also, the Raspberry Pi has a low-resource processor, which more closely resembles the hardware of the EV's or CS's communication controller. The backend processes run on a laptop. All stakeholders are connected to each other via Ethernet. During the charging session, the electric vehicle and the charging station are connected to each other with a modified Ethernet cable allowing 100 Mbps, charging and physical connection detection.

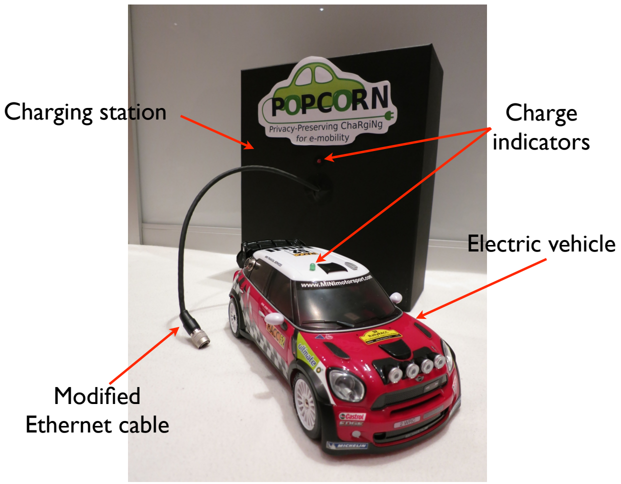

Figure 5: The Proof-of-concept hardware setup.

Results In order to understand how the POPCORN protocol performs on low-resource hardware, the time it takes for the cryptographic operations has been measured [4]. While most operations take a reasonable amount of time (e.g. 8 seconds for signing), creating the contract proof and verifying it takes a long time on the Raspberry Pis, i.e., 90 seconds. The use of non-optimized Java libraries and the Java Virtual Machine on top of the Rasbian operating system largely contribute to this. In a real deployment of POPCORN the computations will be implemented using native code and hardware acceleration. Hence, the software-related speed issues can be ignored. Further, the idle time can be used to prepare the battery management module or the charging can be started before the verification is complete. During a normal charging cycle the charging station requests the vehicle to sign cumulative meter readings. If the vehicle aborts the charging prematurely, the signature is missing for the last charging cycle. If the proof verification takes less time than a charging cycle, the power delivery could already be started while the charging station is still verifying the contract. Then the economic risk is the same as during a charging cycle. A charging session generally takes at least a few minutes, so that an order of magnitude within the few seconds does not affect the overall performance. For fast charging (10 – 30 minutes), the charging station can request a group signature before the power delivery, so that non-repudiation is given when the EV has no valid contract.

Scenarios The proof-of-concept was tested with the following scenarios:

1. *Normal charging:* Including wireless credential updates before charging and payment.
2. *Expired contract:* The contract is expired and the EV tries to charge.
3. *Cheating EP:* The energy provider starts a dispute about an already paid session.
4. *Cheating EV:* During charging, the electric vehicle disconnects the charging cable.

The POPCORN protocol was able to handle all scenarios. The first scenario showed that it is possible to hide anonymous credential attribute values from the issuer, thus offering extra privacy. Scenario 2 showed that the EV is unable to create a contract proof if the contract is expired. In Scenario 3, the dispute resolver ended the dispute after receiving the payment receipt from the mobility operator. Finally, in scenario 4 the charging station directly detects the interruption due of the physical connection detection feature of the modified cable.

The POPCORN evaluation shows that the privacy requirements have been fulfilled and that a fully privacy-preserving electric vehicle charging with contract-based payment is possible. The prototype shows that this can even be implemented on resource-limited hardware.

5. Conclusion

In this work we have highlighted the privacy invasion that electric vehicle charging based on ISO/IEC 15118 may introduce. As our privacy impact assessment of this protocol has shown, drivers may unnecessarily reveal details about their whereabouts to charging station and mobility operators. Using our PIA results, we designed modular enhancements of the protocol based on state-of-the-art PETs, showing that PET technology allows to implement comfortable and fully functional Authentication, Authorization and Accounting (AAA) for eMobility and electric vehicle charging without sacrificing privacy. This claim was corroborated by a second PIA analysis and a prototype implementation.

By taking a modular approach to extend the original ISO/IEC 15118 protocol, POPCORN can even be introduced in a gradual way, if industry is not willing to initially introduce a dispute resolver or payment handler. Of course this goes at a reduced privacy protection. Still it would allow an immediate introduction of better privacy protection to the current protocols and infrastructures. We are in the process of submitting our POPCORN proposal to the respective ISO working group to discuss the potential for actual consideration in the standard.

We have the hope that our work will provide a significant contribution to the introduction of privacy-preserving and still functional and convenient electric vehicle charging infrastructures. At the same time, it provides a lesson how today's PETs in combination with thorough PIA can be used to build and deploy privacy-enhancing systems that introduce only modest additional effort but fully retain system functionality and security.

References

[1] 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.

[2] 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.

[3] Deutsches Institut für Normung. DIN SPEC 91286:2011-11: Electric mobility – Schemes of identifiers for E-Roaming – Contract ID and EVSE ID, Nov 2011.

[4] C.N.Höfer. Popcorn: Privacy-preserving charging for eMobility. Master's thesis, University of Twente, January 2013.

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

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

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

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

[9] Raspberry Pi Foundation. Raspberry Pi - An ARM GNU/Linux box, 2012.

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

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