Communication Reduced Interaction Protocol between Customer, Charging Station, and Charging Station Management System

Karl-Heinz Krempels[1], Christoph Terwelp[1], Stefan Wüller[1], Tilman Frosch[2] and Sevket Gökay[1]
[1]*Information Systems & Databases, RWTH Aachen University, Aachen, Germany*
[2]*HGI, Ruhr-University Bochum, Bochum, Germany*

Keywords: Charging Station, Interaction Protocol, Authentication Protocol, Reduced Communication Effort, QR Code.

Abstract: The emerging build-ups of charging station infrastructures require sufficiently secure and economic authentication protocols. Existing protocols for the purpose of authenticating a customer against a charging station have the inherent disadvantage that they expect a network connection to the management system, produce a communication overhead, or might reveal sensitive customer data depending on the protocol. The protocol, provided by us, enables a multiple-operator customer-to-charging station authentication system. The particularity of the protocol is that it does not require a permanent network connection between charging stations and a corresponding management system, reduces the communication overhead between the involved entities, and protects sensitive customer data at a high rate.

1 INTRODUCTION

The availability of a charging infrastructure is one of the decisive factors for the success of electric vehicles. Thus, one can currently observe significant efforts in Germany and many other countries to expand the existing charging infrastructure. In the course of this expansion, costs must be kept in check. Besides the acquisition costs, installation and maintenance costs should be kept as low as possible. One factor within the operational costs is the need for a continuous communication channel between charging stations and a corresponding charging station management system.

The interaction protocol we propose in this paper enables a dynamic control of charging stations without the necessity of a constant communication channel to a management system. This is achieved by leveraging the Internet connection of the customer's smartphone as a communication channel between charging station and charging station management system for authentication purposes.

The remainder of the paper is organized as follows: In Section 2 we describe authentication protocols for charging stations that are currently in use. Section 3 and 4 provide a detailed description of the our solution and optional protocol extensions. In Section 5, we discuss core design decisions and give a summary of the advantages of our protocol and the provide the possibility to extend its application field in Section 6.

2 RELATED WORK

In the following we present the state of art of protocols used to authenticate customers against charging stations. The major disadvantage of those protocols is the costly communication effort needed before and after each charging process between the charging station and the charging station management system. The interchanged data basically consists of customer's authentication data, information for the adjustment of meter readings, as well as control commands, e.g., the activation of the charging station. Partially, the protocols enable a local authentication by utilizing *whitelists* (OCPP Steering Group, 2012). However, this jeopardizes the confidential customer data which are deposited within the charging station.

Furthermore, the following protocols rely on a network connection, i.e., a network connection is essential for the commissioning of a charging station. Below, we will show that a network connection is not absolutely necessary to fulfill the requirements of those systems.

Krempels K., Terwelp C., Wüller S., Frosch T. and Gökay S..
Communication Reduced Interaction Protocol between Customer, Charging Station, and Charging Station Management System.
DOI: 10.5220/0004971801180125
In *Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems* (SMARTGREENS-2014), pages 118-125
ISBN: 978-989-758-025-3

2.1 Authentication Via RFID-card (OCPP Steering Group, 2012)

The customer owns an RFID-card which enables him to authenticate against a charging station with an integrated RFID-reader. If the read ID appears on the charging station's local whitelist, the user is successfully authenticated against the charging station without involving the charging station management system into the authentication process. Otherwise, if the ID does not appear on the whitelist, there has to be a data exchange between the charging station and the charging station management system. The customer logoff works analogously. Meter readings and control data is communicated using the network connection to the charging management system.

2.2 Authentication Via Plug and Charge (ISO, 2013)

The costumers connects his vehicle with a charging station by a charging cable carried along. The authentication is done in two steps. The charging cable plug is endued with an RFID-chip. If the plug of the charging cable is in an appropriate range the ID is read by the RFID-reader of the charging station. Reading a valid ID induces the charging station to open it's socket. For the second authentication step the communication channel established by the charging cable is used. A certificate which is deposited within the vehicle is used in the underlying protocol to authenticate the customer against the charging station. The charging process is terminated by unplugging the charging cable.

The verification of the authentication data and the exchange of meter readings is ensued via the network connection to the charging station management system.

2.3 Authentication Via Hotline

The customer dials the operator's hotline which is fixed on the charging station and communicates his user ID, password and the charging station ID. A successful verification induces the activation of the charging station for the authenticated customer. The customer logoff works analogously.

Meter readings and control data is communicated using the network connection to the charging management system.

2.4 Authentication Via Internet

The authentication via Internet proceeds analogously to the authentication via hotline. The customer communicates user ID, password, and charging station ID by filling the appropriated form on the website of the charging station operator or using a provided smartphone application for this purpose.

3 THE BASIS PROTOCOL

Before we describe the details of our protocol, we give a concise overview with Section 3.1. The protocol flow is given by the sequence diagrams depicted in Figure 1 and 2. During an initialization phase each charging station (CS) is endued with a public/private key pair (pk_{CS}, sk_{CS}) and the public key(s) of the respective charging station management system(s) (pk_{CSMS_i}), respectively. The charging station management system (CSMS) retains a matching private key and the public key of each charging station. Keys are stored in a non-removable secure storage, from which they cannot be extracted by unauthorized entities. When a new user signs up with a provider, he receives a set of unique credentials to authenticate at the CSMS.

3.1 Protocol Flow

On the push of a button integrated into the CS, it generates a QR code and shows it on its display. The customer scans the QR code using his smartphone and communicates its content in combination with his authentication data to the CSMS. Optionally, the user can provide additional position information using the provided smartphone application, e.g., his GPS coordinates. The CSMS provides the user with authentication information for this CS, which the application on the user's smartphone displays as a QR code. The CS scans this QR code from the phone's display. If the authentication information is valid, it unlocks / enables the power socket. Charging ends when the electric vehicle's battery management signals sufficient charge, the customer presses a button at the CS and presents the QR code again, or the customer manually releases the power cable using a mechanical release device integrated in his vehicle. When charging ends, the CS creates a data tuple to be used for billing and stores it in temper-evident memory. The CSMS periodically tries to connect to every CS. When successful, it recovers all billing data tuples retained within the CS.

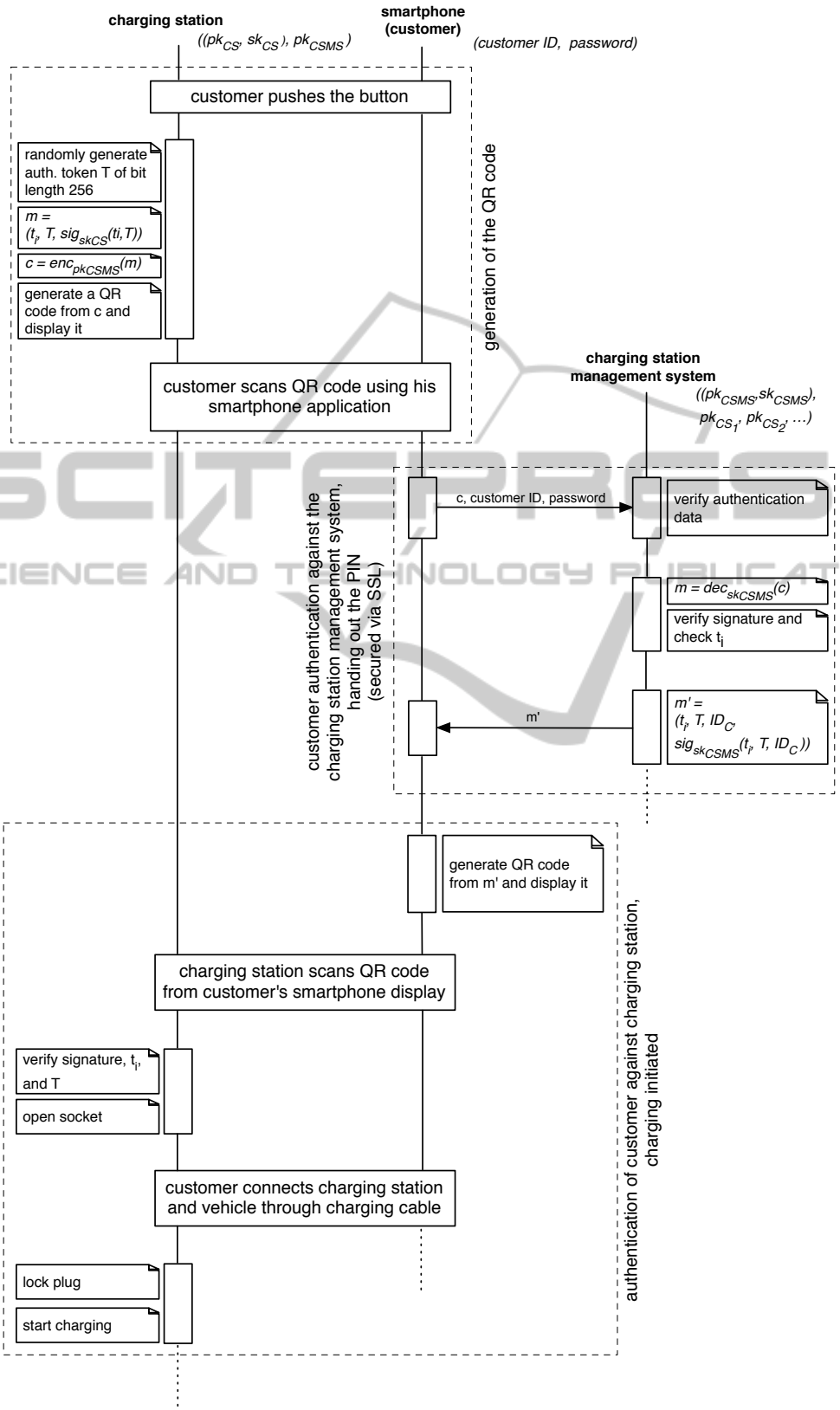

Figure 1: Basis Authentication Protocol (Part 1).

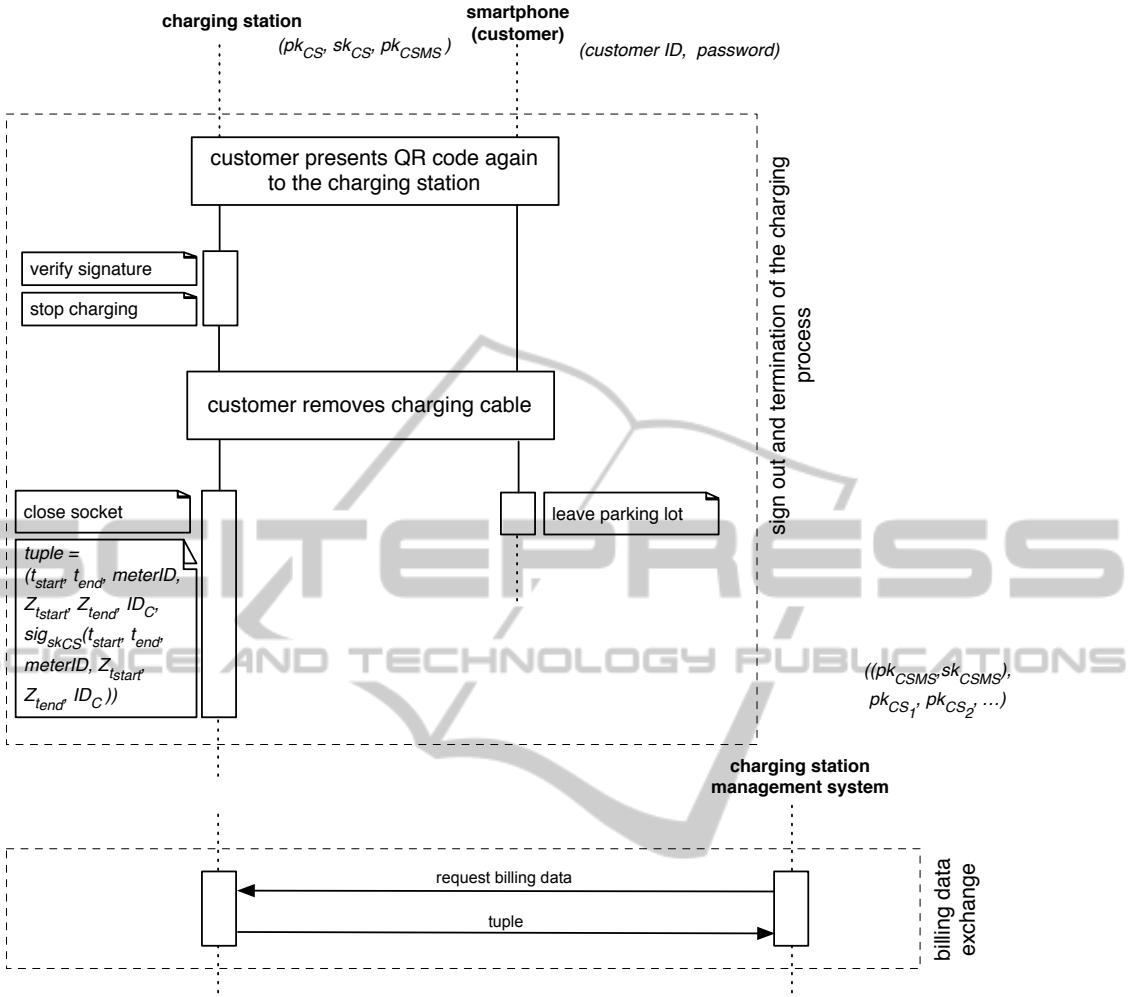

Figure 2: Basis Authentication Protocol (Part 2).

3.2 QR Code Generation

On the push of a button the CS randomly chooses an authentication token T of 256 bit length. It only creates n tokens per time t. n,t are chosen as a compromise between usability and security. Here, usability primarily concerns the fact that each customer willing to use the system should be able to receive an unused token. Under a security perspective one must consider that the source of randomness must not be exhausted or the system overloaded by very frequent pressing of the button, where each button press triggers a set of cryptographic operations that consume system resources.

The CS creates a message $m = (timestamp = t_i, token = T, signature = sig_{sk_{CS}}(t_i, T))$, creates $c = enc_{pk_{CSMS_i}}(m)$, and creates a QR code containing c that it displays to the customer. t_i is a timestamp produced at message creation, in a non-ambiguous time representation. The customer scans this QR code using his smartphone application.

3.3 Customer Authentication

The smartphone application connects to the CSMS using a secure variant of Transport Layer Security (TLS), a cryptographic protocol frequently used to secure a cornucopia of communications on the Internet, e. g., for online banking. We recommend to use TLS-DHE, which has recently been proven to be secure by Jager et al. (Jager et al., 2012).

The user authenticates himself at the CSMS and establishes a secure session. Within this session the application transmits the message c contained in the CS' QR code which the CSMS decrypts and verifies. After successful verification the CSMS checks

whether t_i is within a defined time period to be considered *fresh*. Optionally, the user can provide additional position information using the provided smartphone application, e.g., his GPS coordinates. We discuss this extension in Section 4. The CSMS transmits a message $m' = (timestamp = t_i, token = T, customerID = ID_c, sig_{sk_{CSMS}}(t_i, T, ID_c))$ back to the application. ID_c is a unique identifier for the authenticated customer. The application creates a QR code from m', which the user presents to the CS. The CS scans the QR code and verifies m' and T. If T and the signature over $T, customerID$ is valid, and t_i is within a defined time period, the power socket is unlocked / enabled.

3.4 Storage and Transmission of Billing Data

Upon the end of the charging process, the CS creates a data tuple for billing and ensures its authenticity during transport and storage by means of a digital signature. The tuple is formed as

$$\begin{aligned} tuple = (&t_{start}, t_{end}, meterID, Z_{t_{start}}, Z_{t_{end}}, ID_c, \\ &sig_{sk_{CS}}(t_{start}, t_{end}, meterID, Z_{t_{start}}, Z_{t_{end}}, \\ &customerID)), \end{aligned}$$

where t_{start} is a timestamp recorded upon starting to charge, t_{end} is a timestamp indicating the end of charging, $meterID$ is the unique identification number of the energy meter (if required by local regulation), $Z_{t_{start}}$ and $Z_{t_{end}}$ are the energy meter values at beginning an end of charging, respectively. We chose digital signatures over symmetric methods such as Message Authentication Codes, as both can ensure message integrity and authenticity, but the former can also provide non-repudiability. Non-repudiability is essential to be able to prove that only the respective CS could have created the signed tuple. However, this objective cannot be reached using means of symmetric cryptography.

The CS stores the data tuple in temper-evident memory, such that any attempt to erase a billing tuple can be discovered. The CSMS periodically tries to connect to each CS. Upon successfully establishing a secure connection, it recovers all billing data tuples and stores them centrally, such that they are available for the billing process. When the CSMS has successfully stored and verified a tuple, this tuple is remove from the CS' memory.

4 PROTOCOL EXTENSIONS

In the following we describe further optional extensions to the basis protocol which affect the security of the protocol and the cooperation between different charging station operators.

4.1 QR Code Relay Attack Prevention

We consider the following theoretical attack scenario: An attacker positions a manipulated charging station with the ability to receive QR code data generated by the attacker and to display it to the customer.If an authentication token is read by the manipulated charging station, it has to be transmitted immediately to the attacker whereas an error message is displayed to the customer. An existing connection to the charging network is not necessary to accomplish this task. Utilizing the manipulated charging station to his own authorization process the attacker is enabled to charge his vehicle for free or at the cost of the victim.

The attacker positions his vehicle in front of an authorized charging station, reads the displayed QR code, sends the QR code data to the manipulated charging station (e.g. using an implemented smartphone application for this purpose), and waits until the valid QR code, provided by the customer at the manipulated charging station, is received. If the QR code loses validity during the transmission, the attacker repeats the proceeding with a fresh QR code. In this scenario, the charging station management system provides an authentication token for an authorized customer and connects the billing information to his account. Once the customers presents the QR code to the manipulated charging station, an error message is displayed, informing about a defective and referencing to another charging station. Since the customer cannot distinguish between the authorized and the manipulated charging station, he is not aware of the fact that an attacker positioned at another charging station uses his QR code to charge a vehicle at his cost. Under certain assumptions, this attack can be thwarted by integrating spatial data into the authentication protocol: The mobile application determines the customer's GPS coordinates during authentications. This position is then concatenated to the message c the customer transmits to the charging station management system.

With this protocol extension, the charging station management systems checks if the customer's GPS coordinates match with corresponding charging station's coordinates considering a certain tolerance. Only if this additional condition is satisfied the management systems issues m'. The assumption for this

security feature is that the manipulated and the authorized charging station the attacker uses are sufficiently wide apart from each other exceeding the maximal accepted tolerance.

4.2 Multi-operator Authentication

A simple extension to the basis protocol of Section 3 enables a multi-operator authentication without the necessity of sharing customer data between operators. Each operator obtains an operator ID. Instead of just pressing a button, the customer chooses the operator at the CS. The CS encrypts the message m using the respective operator's public key pk_{CSMS_i} and then incorporates the appropriate operator ID within the QR code in plaintext. Basing on the operator ID, the provided smartphone application decides which operator the authentication message is forwarded to.
Manipulating the operator ID can not harm the system because the assigned operator is not able to decrypt the data which is necessary to return an authentication token to the customer.

4.3 Privacy-preserving Solution

Locational privacy can be defined as 'the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use' (Andrew J. Blumberg and Peter Eckersley, 2009) and has become increasingly relevant with rise of long-term data retention – itself made facilitated by increasingly cheap data storage.

While the solution we presented so far does not preserve a customers location privacy – it allows for the creation of a movement profile based on the spatio-temporal location of each charging process – a limited set of changes can mitigate this threat: Instead of sporadically connecting to the Internet to allow for the CSMS to retrieve billing data, each CS uses this temporary Internet link to connect to the Tor network (Mathewson et al., 2004), such that it is addressable as a location-hidden service. This means, it is known to the CSMS via its `.onion` address, but not via its IP address or physical location. While this may sound far-fetched and impractical in reality, the Tor network is a highly redundant, distributed system that can provide connectivity with sufficient throughput and latency for the application at hand (Frosch et al., 2013). The authenticity and non-repudiation of messages from CS to CSMS does not longer depend on classical signature algorithms. Instead, messages are signed using a group signature scheme, like XSGS (Delerablée and Pointcheval, 2006). Message m will be formed as $(timestamp = t_i, token = T, address = onionaddress_{CS}, signature = gsig(t_i, T, onionaddress_{CS}))$, while c will still be created as $enc_{pk_{CSMS_i}}(m)$. Instead of signing the billing data tuple with a conventional signature, the CS uses the a modified eXtremely Small Group Signature as proposed by Frosch et al. (Frosch et al., 2013).

5 DISCUSSION

In the following we discuss the potential of a completely offline solution, the advantages of using a random binary token over a numeric Personal Identification Number (PIN), as well as, the issue of a trustworthy time source.

5.1 Offline Solution

In the unlikely case that a charging station is located such that it can never access the Internet, small changes can be made to the protocol leverage the user's communication with the CSMS to transport most billing relevant data within. Including the current energy meter value Z_{t_i} in message m, such that $m = (meter = Z_{t_i}, timestamp = t_i, token = T, signature = sig_{sk_{CS}}(Z_{t_i}, t_i, T))$. The charging process can only be terminated by performing the authentication procedure again, such that a message $m_2 = (meter = Z_{t_j}, timestamp = t_j, token = T', signature = sig_{sk_{CS}}(Z_{t_j}, t_j, T'))$ is transmitted to the backend. However, as many electric vehicles come with a manual unlock mechanism for the power connector, even a honest, but curious, customer can evade the transmission of m_2 and thus charge without paying. Additionally, t_i, t_j are created when the customer presses a button and not at the exact time the charging starts. Depending on local legislation, this may not be precise enough.

5.2 Random Token vs. Random PIN

Although numeric PINs are frequently used to authenticated customers, e. g., at automatic teller machines (ATMs), the keyspace of usable-length PINs is very limited. PIN lengths up to 6 digits can be considered acceptable to the customer, as they are used in commercial applications. However, as the character repertoire is limited to $[0..9]$, the keyspace is limited to 10^l. The probability that an attacker guesses a valid password is thus $\frac{1}{10^l}$, i. e., on average an attacker needs $\lfloor \frac{10^l}{2} \rfloor$ guesses. As this limitation is well known, many PIN-based authentication systems require not only the

knowledge of the PIN but also the possession of physical token, e. g., a bank card. Additionally, usability is further reduced by the fact that a customer may only mistype a PIN n times, before the physical token is automatically invalidated or confiscated. n is often chosen as 3.

By choosing a QR code reader as input method to the charging station, instead of a PIN pad, we avoid the usability issue altogether. The user is not forced to enter an arbitrary set of numbers correctly, but simply presents his smartphone to the reader. Thus, we can choose to a much longer knowledge-based authentication token. We choose a binary token of 256 bit length, which results in a keyspace of 2^{256}. This allows for a significantly more secure authentication process and also improves usability as there is no need enforce arbitrary limitation on how often a user may try to enter a credential. Vandalism-proof QR-code readers are widely in use today, e.g., at airport boarding terminals.

5.3 Time Source

We use a timestamp as a freshness parameter in our protocol. However, this implies that we have a trustworthy time source at our disposal. This is also a basic assumption for post-paid systems, as many regulations require to inform the customer when a service or a good has been delivered. When an attacker can trick a CS into assuming a time in the past as being current, he can thus replay an old message m'_{old}, which will be accepted if the CS's time and the message timestamp are within a tolerated interval. Even existing customers can use erroneous system times to their advantage, as the energy provider will have a hard time arguing how it can bill, e.g., for a charging process with at timestamp dating from before the customer ever signed up with this provider.

However, a trusted time source is not easy to come by. DCF-77, the Network Time Protocol (NTP), and GPS are popular time sources. However, none of these protocols provide information on the authenticity of the content and can thus be manipulated. DCF-77 transmitters can be built for very limited costs[1] or even using standard soundcards[2]. NTP packets can be manipulated in the path of communication. Alternatively, DNS entries can be hijacked by an out-of-path attacker (Leyden, 2013), pointing to an NTP server the attacker controls. While Tippenhauer et al. (Tippenhauer et al., 2011) have shown that the spoofing of a GPS signal is feasible, this attack induces significantly higher costs for the attacker than the aforementioned ones. For the time being, GPS should be the preferred time source for outdoor CS installations. In indoor areas, such as parking garages, the GPS time signal can be forwarded via internal network. Alternatively, `tlsdate` (Applebaum, 2013) may provide a coarser, but possibly more secure alternative time source when used as consensus source.

[1] http://endorphino.de/projects/electronics/timemanipulator/index_en.html

[2] http://0x7.ch/text/dcf77.pdf

6 CONCLUSION

We presented a protocol that enables providers to operate charging stations without a continuous communication channel connecting them to the charging station management system. This allows a more economical operation and a higher security of the charging station infrastructure, as the charging station has no privileged access to the backend infrastructure. Involving QR codes enables a multi-operator authentication of the customer against the charging station without any communication between the charging station and the management system and without depositing sensitive data on the charging station.

While we focus on the application of recharging electric vehicles, our solution is flexible and can also be adapted to a wide variety of application fields, such as time-limited access of rental cars, pedelecs, and bicycles.

ACKNOWLEDGMENTS

This work was supported by the German Federal Ministry of Economics and Technology[3]:
(Grant 01ME12052 econnect Germany).
This work was supported by the German Federal Ministry of Economics and Technology:
(Grant 01ME12025 SecMobil).

REFERENCES

Andrew J. Blumberg and Peter Eckersley (2009). On locational privacy, and how to avoid losing it forever. Technical report, Electronic Frontier Foundation.

Applebaum, J. (2013). tlsdate. https://github.com/ioerror/tlsdate.

Delerablée, C. and Pointcheval, D. (2006). Dynamic fully anonymous short group signatures. In *VIETCRYPT*, pages 193–210.

[3] Bundesministerium für Wirtschaft und Technologie (BMWi) http://www.bmwi.de/

Frosch, T., Schäge, S., Goll, M., and Holz, T. (2013). Improving location privacy for the electric vehicle masses. Technical Report TR-HGI-2013-001, Horst Görtz Institute for IT Security.

ISO (2013). Road vehicles - Vehicle to grid communication interface. Technical Report ISO/IEC 15118-1, International Organization for Standardization, Geneva, Switzerland.

Jager, T., Kohlar, F., Schäge, S., and Schwenk, J. (2012). On the security of TLS-DHE in the standard model. In *Advances in Cryptology - CRYPTO*.

Leyden, J. (2013). Avg, avira and whatsapp pwned by hacktivists' dns hijack. http://www.theregister.co.uk/2013/10/08/dns_hijack_attack_spree/.

Mathewson, N., Syverson, P., and Dingledine, R. (2004). Tor: the second-generation onion router. In *Proc. USENIX Security Symp*.

OCPP Steering Group (2012). Open Charge Point Protocol. Technical Report 1.5, e-laad.nl.

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Capkun, S. (2011). On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86. ACM.