MENNEKES Elektrotechnik
GmbH & Co. KG
Aloys-Mennekes-Str. 1
57399 Kirchhundem, Germany
Tel. +49 (0) 27 23 / 41-1
Fax +49 (0) 27 23 / 41-214
E-mail: info@MENNEKES.de
Internet www.MENNEKES.de

Statement

Data Security of the MENNEKES Charging Infrastructure

Kirchhundem, ***01.02.2018*** - Following publications issued by the Chaos Computer Club (CCC) regarding data security when charging electric vehicles, we have receive questions on the security of our charging systems.
Due to the far-reaching media coverage generated by this report, we can fully understand the concerns of our customers and the public. Given the growing electric mobility market, the possibility of cases arising in which attempts are made to take criminal advantage through fake identities or manipulated devices cannot be entirely excluded. As a manufacturer of charging systems, we would like to take this opportunity to summarise the questions that have been raised with us so far and point out which options already exist for operators today to keep their charging processes with MENNEKES charging systems safe and secure.
So, what is this all about?

RFID Cards - Security and Use

The CCC publication highlighted that RFID cards currently in widespread use are not tamper-proof. In the field of electric mobility today, the unique card number of the RFID card (UID - Unique Identifier) is often used for identification at a charging point. The charging point operator or e-mobility provider

MENNEKES Press Contacts:
Joachim See, Marketing & Corporate Communications Manager, e-mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Corporate Communications, e-mail l.baier@MENNEKES.de

uses this RFID card number to assign the charging data to the respective customer.
This UID is the lowest common denominator available to enable customers of different e-mobility providers to use charging stations of different operators and manufacturers. Therefore, in addition to smartphone app authorization, this RFID authentication method is often also required, e.g. as a minimum standard in the current German government funding guidelines of the BMVI (§7.3).

Open Charge Point Protocol

Operators and consumers demand high availability of charging systems. Therefore, the OCPP (Open Charge Point Protocol) communication standard also describes the optional additional use of a local whitelist cache. This safeguards the continuous accessibility of charging stations even in the event of a backend (back office) communication failure.
Unfortunately, due to the potential duplicability of the UID, authentication via RFID card is not completely secure.

What do secure solutions from MENNEKES look like?

Secure alternatives for authentication already exist

1. APP and ad hoc charging

Smartphone app and ad hoc charging solution (charging without a contract or prepaid card), for example, are two such authentication options. Incidentally, both methods are required by the funding guidelines in the German implementation of the EU Alternative Fuels Directive for charging at public charging points.
An e-mobility provider is therefore already able to offer several authorization methods in accordance with the law. The EV driver can choose which method to use.

MENNEKES Press Contacts:
Joachim See, Marketing & Corporate Communications Manager, e-mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Corporate Communications, e-mail l.baier@MENNEKES.de

2. Backend - chargecloud

For the operation of networked charging infrastructure, MENNEKES together with chargecloud GmbH offers a cloud-based software solution including smartphone app and ad hoc charging solution for operating charging points, administering customers and billing charging processes. This system addresses current security aspects, incorporating automatic import of security updates and encrypted data transmission, representing a high degree of data security.

Alternative backend

Operators may also offer their customers other backend systems on the market compatible with MENNEKES charging systems. The providers of these software-based solutions will be able to give further details on the security aspects of their respective systems.

3. Future authentication methods

Other authentication methods, based on encrypted direct data exchange between charging station and electric vehicle, are in the works. These methods will require the charging stations and electric vehicles to be compliant with the ISO 15118 standard and require additional hardware integration.

Mechanical protection against tampering with charging systems

In connection with the paper presented by the CCC, reference was also made to the possibility of data or RFID card numbers being read out on some charging systems on the market.

MENNEKES charging systems in public areas are all protected by security locks and have a very high level of mechanical (intrusion) protection. In the

MENNEKES Press Contacts:
Joachim See, Marketing & Corporate Communications Manager, e-mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Corporate Communications, e-mail l.baier@MENNEKES.de

eventuality that someone with excessive criminal energy managed to gain access to the interior of our devices, the communication gateway and charging point controller are encrypted and password-protected. This combination of mechanical lock and software barrier provides the best possible protection.

For charging systems in private locations, mechanical protection properties may be less stringent. These charging systems are already installed in more secure environments such as garages or other access-protected areas on private property. Although these charging systems may be opened with a tool, it is still necessary to know various passwords and PINs to access the device, charging process and RFID data or to change the device configuration.

Outlook for Plug and Charge

Charging electric vehicles requires a secure communication between the charging infrastructure and the electric vehicle. The upcoming ISO 15118 standard will make this possible in the future. In this standard, charging station and electric vehicle are respectively required to implement standard-compliant protocols in order to communicate with each other. Here, the prerequisite for both sides (charging point / vehicle) is encryption of the data by means of software certificates.
MENNEKES will offer this method in the future.

Summary

The observations of the CCC are fully justified. As a manufacturer of charging systems, MENNEKES implements solutions that are required by the market or by legal regulations and standards. We currently offer three authorization options, with a fourth to be added in the future: RFID, APP, ad hoc and, coming soon, plug and charge.
Ultimately, within the framework of the law, operators and e-mobility providers today can choose which authentication options they want to offer their customers.

MENNEKES Press Contacts:
Joachim See, Marketing & Corporate Communications Manager, e-mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Corporate Communications, e-mail l.baier@MENNEKES.de

In our experience, solutions with a smartphone app and ad hoc access are often offered as an alternative to the RFID card. As a result, the end user (electric car driver) can also decide which method he wants to use.

Electric mobility is evolving rapidly. With the aid of feedback from the market and renowned institutions in addition to the work of the CCC, MENNEKES and its partners will continue to strive to overcome possible obstacles to pave the way for the mobility of the future.

MENNEKES Press Contacts:
Joachim See, Marketing & Corporate Communications Manager, e-mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Corporate Communications, e-mail l.baier@MENNEKES.de