ENSTO

Three ways

to significantly increase your EV charging security

February 2017

Better life.
With electricity.

Secure your charge

Careless security design can leave your EV charging vulnerable to information attacks. EV infrastructure owners looking to improve their business should focus on quality solutions, which are designed to deliver secure EV charging, at all times

For drivers of electric vehicles, the process of EV charging is a simple one: plug in your vehicle to the charging station and use your RFID or mobile app to start the charge. It's easy, just as it should be.

However, careful consideration should be held regarding what goes on behind the process: when dealing with communicating smart chargers, you are inadvertently also in the world of information technology. And in this realm, safety and security are your best friends.

Key things to consider

EV charging becomes vulnerable only if the conditions allow it so. By using unsafe methods – such as a public IP address, or prepaid SIM cards – the user can become vulnerable to attacks, which can have several ramifications:

Identity theft
A degree worse than losing money is losing your user info. The same logic that applies to credit card information: you want it safe for a good reason.

Back-end system penetration
EV chargers often communicate with different back-end systems, such as an eMobility operator. These also need to stay secure in order to eliminate any room for hacking.

Unwanted data consumption
In the case of a safety breach, the user may see a sudden surge in data consumption, directly resulting in loss of money – a surefire indicator that there has been unauthorized hacking.

External / Remote access
Blocking external or remote access to an EV charger is crucial for a secure charging experience. Do not leave the door to your house open – the same goes with EV chargers.

1

2

3

Three ways to significantly increase your EV charging security

While the aforementioned points are important to comprehend, worrying about security in EV charging should never be the user's headache.

The good news is that at Ensto we've taken every measure to design our products as smart and safe as possible – leading to a secure and enjoyable EV charging experience.

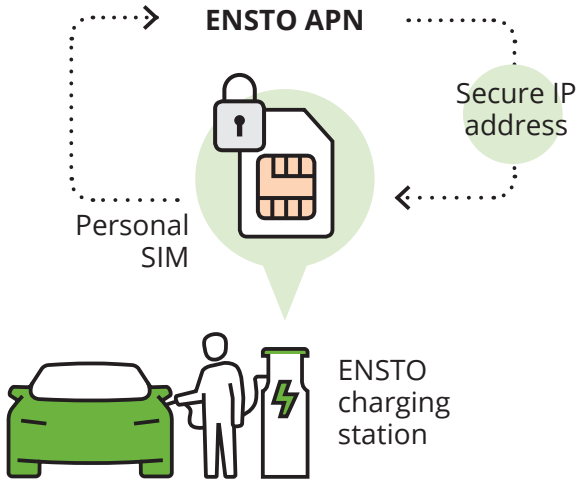
1

Everything stays private

We provide you with your own personal SIM-card, which contacts Ensto's Access Point Network (APN), and receives a private Internal Network IP address.

The two-way communication between the EV charger and back-end systems stays secure via a Virtual Private Network (VPN).

The VPN creates a "tunnel" that enables secure communication between the charging station and its server.



An Access Point Name (APN) is a gateway between a GSM, GPRS, 3G or 4G mobile network, and another computer network.

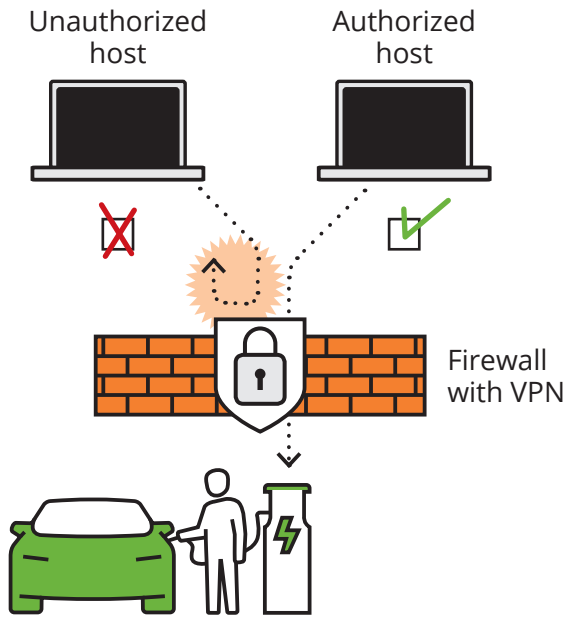
A mobile device making a data connection must be configured with an APN to present to the carrier. The carrier will then examine this identifier to determine what type of network connection should be created, for example: which IP addresses should be assigned to the wireless device, which security methods should be used, and how or if, it should be connected to some private customer network.

2

Eliminate unwanted surprises

Should the user – in any rare instance – misplace or lose his or her SIM card, the operator will freeze the SIM immediately upon the user's request. Depending on the user's request, their SIM card can also be bound to a specific EV charging point.

In addition, the operator will monitor the data traffic in real-time and react by freezing the card if there is any indication of overt data consumption.



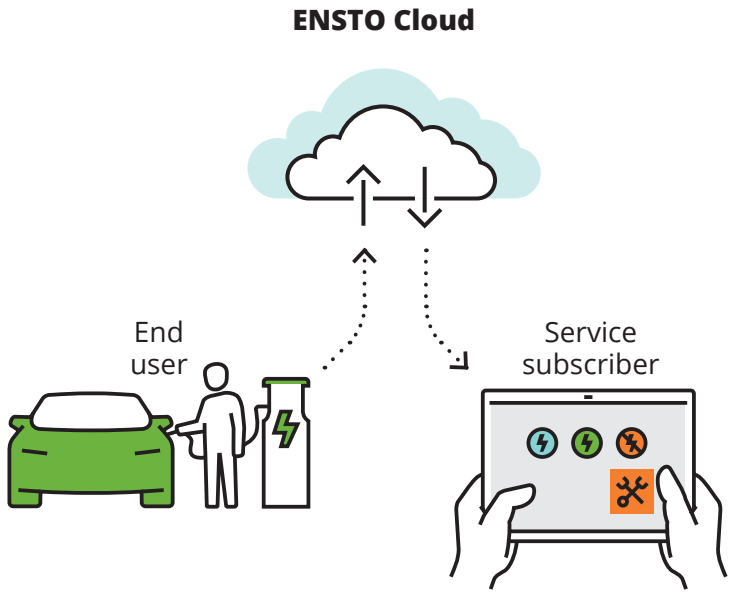
A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN will therefore benefit from the functionality, security, and management of the private network.

3

A protocol for safety

Ensto's EV chargers are OCPP compliant: the global open standard for EV charging equipment management. This protocol means that our chargers are designed to respond only to specific and desired back-end systems – eliminating the chance of misuse or hacking via unmonitored back-ends.

The personal information of the user remains at our partner's commercial back-end. We only cooperate with partners who use every necessary security measure to ensure full safety of information at all times.



The Chago EV Cloud service plays a significant role in providing both the service subscriber and end-user with all the right tools for safe EV charging. We give you a firewalled connection and the latest security updates via Chago EV Cloud, along with any necessary firmware updates to our charging stations.

Another advantage of Chago EV Cloud is its capability for real-time traffic analysis and log backups. You never need to worry about losing your information: it stays safe in the cloud.

ENSTO

About us

Ensto is an international family business which designs and provides smart electrical solutions to improve the safety, functionality, reliability and efficiency of smart grids, buildings and transportation. We are a leading expert in developing and manufacturing high quality charging products and services for electric vehicles, with operations in over 20 countries. Our focus is to support the development of sustainable electric mobility with energy efficient services and reliable, Smart Grid friendly products.

We offer our customers

- Smart and reliable EV charging solutions
- Compatibility with all major EV manufacturers
- Smart Grid ready products and services
- An integration interface to various business systems

Looking to secure your business?

Before you start investing in your EV infrastructure, contact Ensto and we will help you reduce your costs substantially, improve your business case and solidify you as a high-quality player in the market.

www.chago.com