EVBox Livo sets the new *cybersecurity standard.*

WHY IS CYBERSECURITY IMPORTANT FOR EV CHARGING?

EV charging stations, like any other connected device, can be a cyber risk. When connected to your home internet line, an EV charging station can be an access point to your secure personal data; passwords for personal information and accounts, etc.

To manage this risk, having a charging station that protects your personal data is becoming more important than ever.

HOW DO WE PROTECT YOU ?

EVBox Livo sets a new cybersecurity standard for home charging stations. Livo's enhanced cybersecurity is based on automotive standards and utilizes the strictest **OCPP communication profile (profile 3)**.

Our **OCPP 2.0.1** implementation uses TLS to achieve this. The data collected is then stored with a **Trusted Platform Module (TPM) chip**. As a result, EVBox Livo is one of the most secure home charging stations on the market, ensuring full protection of the end-user's data.

TECHNICAL SPESIFICATIONS

OCPP 2.0.1

is the newest communication protocol between a charging station and backend. Of the three security profiles available, EVBox Livo uses the most secure one.

TRUSTED PLATFORM MODULE (TPM)

is the chip which is in the charging station. This encrypts the information in the station.

TLS (TRANSPORT LAYER SECURITY)

is a cryptographic protocol, designed to keep computer communications safe. OCPP 2.0.1 is the first OCPP protocol that supports this additional layer of security.

Find out more about EVBox Livo at evbox.com

KEY BENEFITS

Thanks to EVBox Livo's enhanced cybersecurity capabilities:

01 You can have peace of mind that your data is safe and secure, and can be used in the way you want to.

02 You can rest assured that your home energy network is safe from outside interference.

03 The charging station is hard to access and to be manipulated with.

04 You can soundly use the RFID-charge card on the station, and the data is secured.

Find out more about EVBox Livo at evbox.com