has·to·be eMobility

Certificate-based Authentication of Charging Stations

Whitepaper

2019-12-02

Roland Angerer

has·to·be gmbh
Salzburger Straße 20
A-5550 Radstadt
Reg. Council: Salzburg, Reg.-No. FN 399512 v
VAT: ATU68066335
Managing Director: Martin Klässner
Bank accounts: has-to-be.com/banks

1) Introduction

This whitepaper is intended to detail a way to secure the communication between a charging station and a CPMS (Charge Point Management System) by using a PKI (Public-Key-Infrastructure) to establish trust between the involved parties.

Traditionally charging stations have been connected to a CPMS via some form of secured connection. Typical scenarios include the charging station connecting via a SIM card to a dedicated APN that is itself connected via a VPN to the CPMS infrastructure.

As charging stations become more and more secure and with a widespread adoption of the websocket-based OCPP communication, the need for such a secured infrastructure becomes less significant. Therefore, we want to outline a secure and scalable method to connect charging stations with a CPMS by utilizing well established PKI mechanisms. While this concept is mainly targeted at websocket-based OCPP communication it may also be applicable for other scenarios.

2) Prerequisits

In order to implement the process outlined below we need to have the following in place

- Hardware Manufacturer CA (Certificate Authority) to sign initial charging station certificate
- CPMS CA to sign CPMS charging station certificate

3) Initial Authentication (secured by hardware manufacturer)

When the charging station connects to a CPMS for the first time it is important for the CPMS to be able to establish if the client is indeed a trustworthy charging station. While this could be verified by entering a PSK (pre-shared key) in both systems there is a more elegant and scalable solution: we use a charging station certificate signed by the hardware manufacturer to establish that the charging station is indeed a trustworthy charging station.

During the production of the charging station it is provisioned with a charging station key pair. The corresponding public key will be signed by the hardware manufacturer CA using a validity period that matches the usual lifecycle of the corresponding hardware. The resulting charging station **hardware manufacturer certificate** can be used by the charging station as a TLS client certificate to connect to the CPMS. The CPMS can verify the certificate chain (against the hardware manufacturers root certificate in its certificate store) and might use additional checks like OCSP (Online Certificate Status Protocol) or CRL (certificate revocation list) for added security.

4) Regular Authentication (secured by CPMS)

After the CPMS was able to establish trust in the charging station via the charging stations hardware manufacturer certificate it is recommended to provision the charging station with a certificate that is issued and maintained by the CPMS.

Therefore, the CPMS will trigger a CSR (certificate signing request) on the charging station so the charging stations public key can be signed by the CPMS CA using a shorter validity period for enhanced security. The resulting **CPMS certificate** can then be used as a TLS client certificate by the charging station to initiate future TLS connections to the CPMS. Before the validity of the charging stations CPMS certificate expires it needs to be renewed with another CSR. This process can either be triggered by the charging station or the CPMS as part of the certificate maintenance automation within the CPMS. Refer to the *OCPP 2.0 Specification – Section A. Security* for a detailed explanation on how to use OCPP 2.0 to support the corresponding certificate management.

5) CPMS Authentication

While this document focuses on authentication of the charging station it is also important for the charging station to establish a secure and trustworthy connection to the CPMS. Therefore, the charging station could either be provisioned with CPMS server certificates during production or the corresponding certificate can be set during the CPMS configuration along with the corresponding endpoint URL. Once the charging station is under the control of the CPMS it is recommended to allow the CPMS to manage the CPMS server certificate along with other trust anchors (like the V2G root).