Secure connection

Alfen Charging Equipment

Implementation guide

CONTENTS

1. SECURE COMMUNICATION

1.1 Secure communication

This chapter will describe how to implement basic or secure communication between a charging station and the back office.

This document assumes that an established connection between charging station and back office already exists.

1.1.1 Preconditions

The following conditions should be in place to support secure communication between charging station and back office:

- An established connection between charging station and back office
- OCPP 1.6 SE implemented in back office
- This manual is applicable for charging stations with firmware **4.5.x or higher**
- When configuring with the Service Installer App, **version 3.4.5-115 or higher** is needed

1.1.2 SecurityProfile parameter

SecurityProfile is a configuration parameter introduced in the OCPP 1.6 Security Extension white paper[1] (later referred to as *OCPP 1.6 SE*). We will use this configuration parameter as a reference, but the implementation of OCPP 1.6 SE is only necessary for *Level 3 security*. Using a higher security level than defined by *SecurityProfile* is always permitted.

For example, using security level 1 only ensures that the security must *at least* use basic authentication, but may consist of server authentication too.

If the back office has not implemented OCPP 1.6 SE, then the configuration parameter *SecurityProfile* can be ignored and security level 3 is not (currently) configurable.

Table 1 shows the possible values for the *SecurityProfile* parameter as defined by OCPP 1.6 SE.

Table 1: Possible values for the *SecurityProfile* parameter

Description	Value	Charging station authentication	Central System Authentication	Communication Security
Default	0	*	*	*
Unsecured Transport with Basic Authentication	1	HTTP Basic Authentication	-	-
TLS with Basic Authentication	2	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)
TLS with Client Side Certificates	3	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)

WARNING

The desired security implementation should be tested before the SecurityProfile level is increased. This is to ensure that an invalid configuration can be repaired via the back office rather than requiring scheduled maintenance from a service engineer.

NOTICE

If the SecurityProfile level is higher than '0' (Default), then *UpdateFirmware* request may no longer be used by the back office as it is replaced by *SignedUpdateFirmware*.

1.1.2.1 Level 0, default

Level 0 is the default SecurityProfile level.

For backwards compatibility any security method may be used here. No minimum security implementation is expected, thus an unsecure configuration is allowed for this security level. All Alfen charging stations are configured to use this security profile level by default to ensure security is not *enforced* (as that would break functionality for existing charging stations).

1.1.2.2 Level 1, basic authentication

The minimum security for this level is basic authentication.

No certificates are used in this security configuration nor is the communication channel encrypted. The back office password (*AuthorizationKey* as defined by OCPP 1.6, but also referred to as the *back office authentication key*) is transmitted in plain text.

[1] Otherwise known as *Enhanced security for OCPP 1.6 and Improved security for OCPP 1.6-J*.https://www.openchargealliance.org/news/enhanced-security-for-ocpp-16/

1.1.2.3 Configure level 1 via the Service Installer App

NOTICE

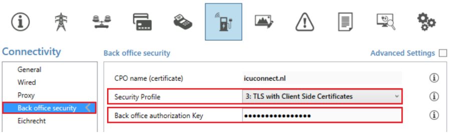
This setting can only be configured with an Admin or Service account.

Configuration of this security level can be done by providing a password in the *AuthorizationKey* parameter (a write only setting in the back office). This is the password that the charging station will use to authenticate itself to the back office as defined by RFC-7617[2] (specifically *Section 2: The 'Basic Authentication Scheme'*).

The back office should be configured to accept solely this password for incoming connections for this charging station. Once the connection is verified to be working, the *SecurityProfile* can be changed to *Level 1 (Basic Authentication)*, but this is only necessary if OCPP 1.6 SE is implemented by the back office.

The configured password is automatically used if the back office responds to the charging station's HTTP request with HTTP status code *401: Unauthorized*.

The configuration parameter *Back office authorization Key* can be found under the *Connectivity* tab in the category *Back office security*. The configuration parameter *Security Profile* can be found in the same location.



CPO name (certificate): icuconnect.nl

Security Profile: 3: TLS with Client Side Certificates

Back office authorization Key: ••••••••••••••••

Figure 1.1: Configuration parameters Service Installer App

1.1.2.4 Configure level 1 via the Back office

Configuration via the back office can be done by sending a *ChangeConfiguration* request with parameter *AuthorizationKey*. The value of this parameter must be sent as a hexadecimal string with a required minimum length of 32 and a maximum length of 40. The charging station shall only reply with *Accepted* if the password is accepted and used.

1.1.2.5 Level 2, server side certificates with basic authentication

The minimum security for this level is basic authentication with server side certificate. The communication is secured using TLS 1.2.

Level 1 security must already be configured before continuing to implement level 2 security as this requires a back office authentication key to be configured.

The charging station uses the CA root certificate of the back office to validate the server certificate chain (as sent by the back office). The initial CA root certificate must be installed using a secure channel. For this purpose a firmware upgrade file (*.fwi) containing the CA root certificate must be created by Alfen. This FWI can safely be used for as many charging stations as desirable. The FWI only changes the configuration and will not alter the firmware itself.

Another method to provide the initial certificate will be implemented at a later point in time. This will allow installation of the initial CA root certificate via the ACE Service Installer without requiring an FWI. The CA server root certificate will automatically be used if the back office URL specifies that protocol WSS (Secure WebSocket) is used. This can be verified by checking that the back office URL is prepended by *wss://*.

WARNING

The CPO (charge point operator) is responsible for installing a new CA root certificate before the current one expires.

Alfen supports the following cipher suites:

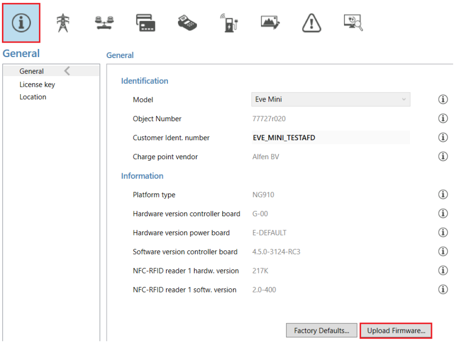
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA (not recommended and could be removed in future firmware releases)

Any cipher suite using EC (Elliptic Curve) and/or DHE (Diffie-Hellman) is currently not supported.

1.1.2.6 Configure level 2 via the Service Installer App

The FWI with CA server root certificate can be sent to the charging station with the *Upload Firmware* functionality in the *General* tab of the ACE Service Installer.

[2] https://tools.ietf.org/html/rfc7617



General

Identification

Model	Eve Mini
Object Number	77727r020
Customer Ident. number	EVE_MINI_TESTAFD
Charge point vendor	Alfen BV

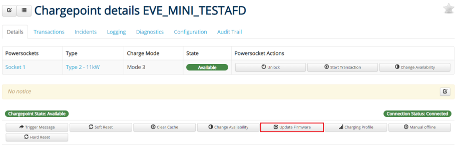
Information

Platform type	NG910
Hardware version controller board	G-00
Hardware version power board	E-DEFAULT
Software version controller board	4.5.0-3124-RC3
NFC-RFID reader 1 hardw. version	217K
NFC-RFID reader 1 softw. version	2.0-400

Figure 1.2: Update firmware button in Service Installer App

1.1.2.7 Configure level 2 via the back office

The FWI with CA server root certificate can be sent to the charging station by means of an *UpdateFirmware* request. Note that this is only permitted when the SecurityProfile is set to '0', otherwise a *SignedUpdateFirmware* must be used.



Chargepoint details EVE_MINI_TESTAFD

Powersockets	Type	Charge Mode	State	Powersocket Actions
Socket 1	Type 2 - 11kW	Mode 3	Available	

No notice

Chargepoint State: Available

Connection Status: Connected

Figure 1.3: Update firmware button in Alfen Connect back office

1.1.2.8 Level 3, server and client side authentication

The minimum security for this level is client and server authentication by means of certificates. Security level 2 must be working before continuing onto level 3.

The CA root certificate installed for security level 2 is used by the CPO to generate a client certificate. For this reason, the CA root certificate is usually a self-signed certificate created by the CPO or back office. Because the CA root certificate was already installed when configuring level 2 security, only the client certificate must be configured.

1.1.2.9 Configure level 3 via the Service Installer App

It is currently not possible to configure a client certificate via the ACE Service Installer. This may change at a later point in time.

1.1.2.10 Configure level 3 via the Back office

This functionality is defined by OCPP 1.6 SE and the required messages must be implemented by the back office to be able to use this.

To configure the charging station to use client authentication:

1. The configuration parameter CpoName is filled with a valid value (name of the CPO or a trusted organisation).This value will be placed in the 'Organisation' part of the 'Subject' field in the Certified Signing Request (CRSR) that the charging station generates.
2. The back office initiates an *ExtendedTriggerMessage* request with *SignChargePointCertificate* as requestedMessage.
3. The charging station generates a public/private key pair and creates a Certificate Signing Request. This is sent to the back office by means of the *SignCertificate* request.
4. The charging station expects the back office to send a *CertificateSigned* request with a valid client certificate.
5. The charging station will validate that the client certificate (chain) is valid before it starts using the certificate.

2.1 Updating CA root certificate

It is possible that the private key used to generate the client certificate by the CPO / back office is leaked or lost. In this case, it might be necessary to update the CA server root certificate. This can be done in one or two ways. If the back office has implemented OCPP 1.6 SE, then it can simply send an *InstallCertificate* request with a new CA root certificate that is signed by the previous CA root certificate.

If this functionality is not available, then a *SignedUpdate-Firmware* request is another option. This requires a new FWI file to be created by Alfen for the new CA root certificate. Updating the CA root certificate via the Service Installer App can be done in the same way (by utilizing the *Upload Firmware* functionality with the new FWI file).