Staying Ahead: OCPP 1.6

OCPP 1.6 Deployment Procedures for Tritium Veefil Charge Points

Version 1

Technical White Paper

17 October 2017

Brisbane, Australia

http://www.tritium.com.au

Contents

1 Overview

This document covers recommended procedures and technical details for charge point operators on how to deploy or upgrade to version 1.6 of the Open Charge Point Protocol (OCPP) on Tritium Veefil charge points.

The intended audience is technical staff at charge point operators who operate and integrate with OCPP server-side infrastructure. This document is also relevant to technical staff responsible for information-security aspects of such infrastructure.

2 Background

The Open Charge Point Protocol (OCPP) is a universal open communication standard for charge point operators to control and monitor their charge-point infrastructure. Charge points manufactured by Tritium Pty. Ltd. have supported this protocol at version 1.5 for many years.

2.1 OCPP version 1.6

The Open Charge Alliance, the body that curates the OCPP specification, released version 1.6 of the protocol in 2015. This version provides a range of improvements over version 1.5 that make it attractive to upgrade to the newer version:

- Better control over charge-point behavior when offline.
- Additional information on the status and potential error conditions on charge points.
- Persistent, authenticated connections between charge points and central system servers via WebSockets.
- Simplified, more compact message format through JSON.

2.2 OCPP 1.6 on Tritium charge points

Tritium charge points support the full spectrum of OCPP 1.6 functionality.

To exploit the support for persistent connections, Tritium charge points only implement the OCPP-J 1.6 flavor of the protocol, based on JSON-formatted messages over WebSockets. Specifically, they require the central system (CS) to support TLS, as per Section 6.2.1 of the OCPP-J 1.6 specification. As an extension on the specification, the server certificate must be signed by a standard Certificate Authority and charge points support all standard key algorithms and sizes on the CS server side. Charge points also use HTTP basic authentication to authenticate at the CS, as per the OCPP-J 1.6 specification, Section 6.2.2.

Tritium charge points do not support OCPP-S 1.6 based on SOAP messages.

3 Deployment considerations

The OCPP-J 1.6 specification addresses a wide range of aspects relevant to implementing the protocol between charge points and central system servers. However, the specification does not clarify certain operational details that charge-point manufacturers and operators need to agree on, in particular it does not cover questions regarding the upgrade of existing charge points from protocol version 1.5 to 1.6 and the deployment of new charge points supporting OCPP-J 1.6:

- How does an operator set the CS connection URL for OCPP-J 1.6 connections?
- How does an operator initialize the authentication between charge points and the central system?

These questions affect both the deployment of new charge points and the migration of existing charge points from protocol version 1.5 to 1.6.

In general, these issues must be addressed with security in mind to prevent unauthorized access to communication between CP and CS. This is a challenge when OCPP 1.5 is used to upgrade to OCPP 1.6 because connections are not necessarily cryptographically authenticated and encrypted. However, for the protocol upgrade procedure documented here, those connections are considered trustworthy in the sense that operators trust them for controlling charge points.

3.1 Configuration of connection URL

This section documents how charge-point operators configure charge-points with the connection URL of their OCPP-J 1.6 central system servers.

3.1.1. Existing deployments

For charge points in the field currently using OCPP 1.5, operators set the connection URL for their OCPP-J 1.6 servers via an OCPP 1.5 *Change Configuration* message with the key *OcppConnectionURL*.

The value must have the format *wss://<hostname>[:<port>]/[<path>]*, for example, *wss://ocpp.example.net/ocpp/1_6/*.

The protocol field must be *wss* (as opposed to *ws*) because the OCPP-J 1.6 client on Tritium charge points only supports TLS connections.

The hostname is the DNS host name or IP address of the server implementing the OCPP-J 1.6 CS.

The port number is optional and defaults to 443.

The path is optional.

3.1.2. New deployments

On charge points delivered with support for OCPP-J 1.6 and no support for OCPP 1.5, the connection URL is preconfigured. Charge point operators supply it to Tritium as part of the initial configuration information applied to charge points during the manufacturing process.

3.2 TLS support

Tritium charge points support OCPP-J 1.6 over plain WebSockets and over TLS. Tritium strongly recommends the use of TLS to ensure confidentiality and the authenticity of the central system.

Charge points honor the protocol (ws or wss) specified in the connection URL configuration parameter. Only if the configured connection URL indicates the wss protocol, the CP establishes a TLS connection.

In the case of TLS connections, Tritium charge points authenticate the central system via TLS certificates. The CP establishes an OCPP-J 1.6 connection only if the CS presents a TLS certificate that meets the following criteria:

- The Common Name (CN) matches the host name as per the configured connection URL
- The certificate is issued by a Certificate Authority registered in the ca-certificates package of the current stable Debian Linux distribution
- The certificate is not expired

Therefore, Tritium charge points do not accept self-signed server certificates.

3.3 HTTP basic authentication and password initialization

Tritium charge points implement HTTP basic authentication as per Section 6.2.2 of the OCPP-J 1.6 specification. This includes support for the CS to set the password over OCPP 1.6, as covered in the specification. The plain WebSocket protocol *ws*, transmits the password of the charge point in the clear to the central system. Tritium therefore strongly recommends the use of the *wss* protocol to protect the confidentiality of the password via TLS.

Charge-point operators have two main options to handle authentication when upgrading or on-boarding charge points for OCPP-J 1.6:

1. The central system does not authenticate a new charge point when it first connects. Specifically, the CS does not require the CP to send an Authorization header in its HTTP requests and ignores the header value if it is sent. After the initial connection is established, the CS sets a password on the CP via the OCPP ChangeConfiguration message and from then on requires the CP to authenticate with that password.
2. The charge point is configured with an initial password. This initial password is transmitted to the central system via a separate channel and the CS requires the CP to authenticate with that password on its first connection. The CS may then change the password as above.

When choosing one of these two options, the operator must weigh up their advantages and disadvantages. The first option is easier to implement than the second. However, it also allows third parties to impersonate charge points during the initial connection. Whether this risk is relevant to the charge point operator heavily depends on external factors outside of the scope of this document.

The first option can be implemented by operators without coordination with Tritium. The rest of this section covers how Tritium facilitates the second option.

3.3.1. Authentication on first use

This section is only relevant to operators who want their central system to authenticate a charge point even on the very first OCPP-J 1.6 connection, before a new password has been set.

Tritium charge points automatically generate strong and unique initial passwords. A charge point stores its initial password locally. The password itself does not leave the charge point over any communication channel. Therefore, the only way for an adversary to obtain the password in plain text is to gain access to the charge point.

A charge point password is used for HTTP basic authentication on the central system. It is a best practice for HTTP basic authentication to store client passwords in the form of hashes instead of plain-text passwords. Even if a third-party learns the password hashes, the hashing ideally prevents them from learning the plain-text passwords. This in turn prevents them from authentication as and impersonating a charge point.

Therefore, charge-point operators are provided with the hash of the initial OCPP-J 1.6 password of each charge point. These hashes are provided in a format that can be integrated directly with the mechanisms for HTTP basic authentication of industry-standard web servers. The charge point generates the following standard hashes for the same initial password:

- Apache md5, salt ID *$apr1$*
- Apache bcrypt, salt ID $2y$
- Glibc sha256, salt ID *5*

The choice of these hashes is a tradeoff between availability in common web servers, security, and performance.

Note that only the *initial* password is available in hashed form over OCPP 1.5 or the Veefil portal. Passwords set by central systems over OCPP 1.6 cannot be accessed over any standard communication channel, neither in plain-text nor in hashed form.

3.3.2. Existing deployments

Charge points in the field currently using OCPP 1.5 generate the initial password for OCPP 1.6-J and its hashes after the connection URL is set via OCPP 1.5 as described above. After the CS has set the connection URL, it may retrieve the password hashes by sending a *GetConfiguration* message with the keys *AuthorizationKeyMd5*, *AuthorizationKeyBcrypt*, and *AuthorizationKeySha256*.

3.3.3. New deployments

For new charge points that use OCPP-J 1.6 only, there is no trustworthy communication channel between the charge point and the CS to communicate the password hashes over. Therefore, the password hashes are made available via the Tritium Veefil customer portal. Since the portal is password protected, unauthorized third parties are unable to access the password hashes. The password hashes are available as .csv and htpasswd files.

3.3.4. Configuring HTTP basic authentication

After the password hashes are obtained, the operators of the CS configure the HTTP basic authentication mechanism of the CS with the most suitable of the password hashes. For Apache, nginx, and similar web servers, this would be achieved by adding a line in the format *<charge point ID>: <password hash>* to an htpasswd file. This allows to authenticate charge points as per the OCPP-J 1.6 specification.

4 Recommended procedures

4.1 Upgrade charge points from OCPP 1.5 to 1.6

The operator of a Tritium charge point in the field can upgrade it from OCPP 1.5 to OCPP 1.6j with the following procedure:

1. Send a ChangeConfiguration message with the key OcppConnectionURL over OCPP 1.5 to the charge point to set the connection URL of the operator's OCPP-J 1.6 central system.
2. Determine which type of password hash is required by the HTTP basic authentication mechanism on the OCPP-J 1.6 central system.
3. Send a GetConfiguration message with the key AuthorizationKeyMd5, AuthorizationKeyBcrypt, or AuthorizationKeySha256 over OCPP 1.5 to the charge point to retrieve the password hash of the charge point.
4. Integrate the password hash with the HTTP basic authentication mechanism on the OCPP-J 1.6 central system.
5. Update the charge point firmware to a version that has been indicated by Tritium Pty. Ltd. to support OCPP-J 1.6.
6. After the charge point is connected to and successfully authenticated against the OCPP-J 1.6 server, set a new password via OCPP-J 1.6 as per the specification. This step is optional from a security perspective since the initial password is unique, has high entropy, is stored only on the charge point, and is not known to any third party, including Tritium Pty. Ltd.

It is possible, but highly discouraged, to skip steps 2-4. In that case, the OCPP-J 1.6 server would have to accept the initial connection from the charge point without password authentication. The risk of this approach is that any third party that knows the connection URL can impersonate an unconfigured charge point, as noted in Section 6.2.2 of the OCPP-J 1.6 specification.

4.2 Deploy OCPP-J 1.6 charge points

New charge points that are supplied by Tritium Pty. Ltd. with OCPP-J 1.6 only support come pre-configured with the connection URL for the central system. To reliably authenticate a charge point from its very first connection, the following procedure is required:

1. Determine which type of password hash is required by the HTTP basic authentication mechanism on the OCPP-J 1.6 central system.
2. Log in at the Tritium Veefil customer portal and retrieve the appropriate password hash of the charge point(s) to be deployed.

3. Integrate the password hash with the HTTP basic authentication mechanism on the OCPP-J 1.6 central system.
4. Start the charge point.
5. After the charge point is connected to and successfully authenticated against the OCPP-J 1.6 server, set a new password via OCPP-J 1.6 as per the specification. This step is optional from a security perspective since the initial password is unique, has high entropy, is stored only on the charge point, and is not known to any third party, including Tritium Pty. Ltd.

As in the upgrade case, it is possible, but highly discouraged, to skip steps 1-3. In that case, the OCPP-J 1.6 server would have to accept the initial connection from the charge point without password authentication. The risk of this approach is that any third party that knows the connection URL can impersonate an unconfigured charge point, as noted in Section 6.2.2 of the OCPP-J 1.6 specification.

5 Summary

This document illustrates recommended procedures for charge-point operators to securely set up OCPP-J 1.6 with new and existing Tritium Veefil charge points. For any additional support, please raise a Veehelp ticket through your Tritium Customer Service account.