OPEN
CHARGE
ALLIANCE

Improved security for OCPP 1.6-J

edition 3 FINAL, 2022-02-17

OCA white paper:

Improved security for OCPP 1.6-J.

Relevant for OCPP 1.6-J (JSON over WebSockets)

Version History

VERSION	DATE	AUTHOR	DESCRIPTION
1.3 Edition 3	2022-02-17	Franc Buve (*OCA*) Paul Klapwijk (*OCA*)	Clarified the description of the certificateHashData fields
1.2 Edition 2	2020-03-31	Paul Klapwijk (*OCA*) Milan Jansen (*OCA*) Robert de Leeuw (*ihomer*)	Edition 2, based on the security fixes in the OCPP 2.0.1 specification
1.0	2018-11-20	Robert de Leeuw (*IHomer*)	Final release after last rework check

1. Scope

This white paper describes how the security enhancements, introduced in OCPP 2.0, can be used, on top of OCPP 1.6-J, in a standardized way.

The security part of OCPP 2.0 was developed to strengthen and mature the future development and standardization of OCPP. It is based amongst others on the end-to-end security design by LaQuSo [11]. Security requirements are included, on security measures for both Charge Point and Central System, to help developers build a secure OCPP implementation.

This document contains the following security improvements:

- Secure connection setup
- Security events/logging
- Secure firmware update

1.1. Edition 3

This document is the Edition 3 of "Improved security for OCPP 1.6-J" white paper. The difference between Edition 3 and the previous version is the clarification of the fields of the CertificateHashDataType, see also the changelog edition 3. This clarification was needed since in practice it turned out that the current description was ambiguous and could lead to non-interoperable implementations, because content and representation were not clearly specified.

Edition 3 of this document replaces previous versions. OCA advises implementers of OCPP 1.6-J to no longer implement previous versions of this document and only use edition 3 going forward.

As a rule, existing numbered requirements are only updated or removed, previously used requirements numbers are never reused for a totally different requirement.

1.2. Security Objectives

This section is informative.

OCPP security has been designed to meet the following security objectives:

1. To allow the creation of a secure communication channel between the Central System and Charge Point. The integrity and confidentiality of messages on this channel should be protected with strong cryptographic measures.
2. To provide mutual authentication between the Charge Point and the Central System. Both parties should be able to identify who they are communicating with.
3. To provide a secure firmware update process by allowing the Charge Point to check the source and the integrity of firmware images, and by allowing non-repudiation of these images.
4. To allow logging of security events to facilitate monitoring the security of the smart charging system.

1.3. Design Considerations

This section is informative.

This document was designed to fit into the approach taken in OCPP. Standard web technologies are used whenever possible to allow cost-effective implementations using available web libraries and software. No application layer security measures are included. Based on these considerations, OCPP security is based on TLS and public key cryptography using X.509 certificates. Because the Central System usually acts as the server, different users or role-based access control on the Charge Point are not implemented in this standard. To mitigate this, it is recommended to implement access control on the Central System. To make sure the mechanisms implemented there cannot be bypassed, OCPP should not be used by qualified personnel performing maintenance to Charge Points locally at the Charge Point, as other protocols may be used for local maintenance purposes.

1.4. OCPP-J Only

This section is informative.

This document is for OCPP 1.6-J (JSON over WebSockets) only, OCPP-S (SOAP) is NOT supported. This document was started, as it is seen as a simple step to port OCPP 2.0 security to OCPP 1.6. But as OCPP 2.0/2.0.1 only supports JSON over WebSockets (not SOAP), this document is also written for OCPP 1.6-J only. Adding SOAP to this document would have taken a lot of work and review by security experts.

1.5. General documentation remarks

This section is informative.

This document is based on OCPP 2.0.1. To help developers that are implementing both 1.6J security improvement and OCPP 2.0.1, we have kept the Use Case numbering from OCPP 2.0.1. So when implementing for example Use Case N01, it is the same use case in this document as in the 2.0.1 specification.

1.6. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [13], subject to the following additional clarification clause:

The phrase "valid reasons in particular circumstances" relating to the usage of the terms "SHOULD", "SHOULD NOT", "RECOMMENDED", and "NOT RECOMMENDED" is to be taken to mean technically valid reasons, such as the absence of necessary hardware to support a function from a Charge Point design: for the purposes of this specification it specifically excludes decisions made on commercial, or other non-technical grounds, such as cost of implementation, or likelihood of use.

1.7. References

Table 1. References

REFERENCE	DESCRIPTION
[1]	ENISA European Network and Information Security Agency, Algorithms, key size and parameters report 2014, 2014. (last accessed on 17 January 2016) https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
[2]	Cooper, D., et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, Request for Comments 5280, May 2008, http://www.ietf.org/rfc/rfc5280.txt
[3]	Dierks, T. and Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.2, Internet Engineering Task Force, Request for Comments 5246, August 2008, http://www.ietf.org/rfc/rfc5246.txt
[4]	Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, May 2004. https://www.ietf.org/rfc/rfc3749.txt
[5]	Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013. (in German) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html
[6]	Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, September 2005. https://www.ietf.org/rfc/rfc4210.txt
[7]	National Institute of Standards and Technology. Special Publication 800-57 Part 1 Rev. 4, Recommendation for Key Management. January 2016. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final
[8]	RFC 2617. HTTP Authentication: Basic and Digest Access Authentication. https://www.ietf.org/rfc/rfc2617.txt
[9]	RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://www.ietf.org/rfc/rfc5280.txt
[10]	OCPP 1.6. Interface description between Charge Point and Central System. October 2015. http://www.openchargealliance.org/downloads/
[11]	Eekelen, M. van, Poll, E., Hubbers, E., Vieira, B., Broek, F. van den: An end-to-end security design for smart EV-charging for Enexis and ElaadNL by LaQuSo1. December 2, 2014. https://www.elaad.nl/smart-charging-end2end-security-design/
[12]	RFC 2818. HTTP Over TLS. https://tools.ietf.org/html/rfc2818
[13]	Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997. http://www.ietf.org/rfc/rfc2119.txt
[14]	RFC 2986. PKCS #10: Certification Request Syntax Specification, Version 1.7. https://www.ietf.org/rfc/rfc2986.txt
[15]	RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, https://www.ietf.org/rfc/rfc6960.txt

2. Secure connection setup

2.1. Security Profiles

This section defines the different OCPP security profiles and their requirement. This White Paper supports three security profiles:
The table below shows which security measures are used by which profile.

Table 2. Overview of OCPP security profiles

PROFILE	CHARGE POINT AUTHENTICATION	CENTRAL SYSTEM AUTHENTICATION	COMMUNICATION SECURITY
1. Unsecured Transport with Basic Authentication	HTTP Basic Authentication	-	-
2. TLS with Basic Authentication	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)
3. TLS with Client Side Certificates	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)

- The Unsecured Transport with Basic Authentication Profile does not include authentication for the Central System, or measures to set up a secure communication channel. Therefore, it should only be used in trusted networks, for instance in networks where there is a VPN between the Central System and the Charge Point. For field operation it is highly recommended to use a security profile with TLS.

2.2. Generic Security Profile requirements

Table 3. Generic Security Profile requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.001		The Charge Point and Central System SHALL only use one security profile at a time
A00.FR.002	If the Charge Point tries to connect with a different profile than the Central System is using	The Central System SHALL reject the connection.
A00.FR.003	If the Charge Point detects that the Central System has accepted a connection with a different profile than the Charge Point is using	The Charge Point SHALL terminate the connection.
A00.FR.004		The security profile SHALL be configured before OCPP communication is enabled.

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.005		Lowering the security profile that is used to a less secure profile is, for security reasons, not part of the OCPP specification, and MUST be done through another method, not via OCPP. OCPP messages SHALL NOT be used for this (e.g. ChangeConfiguration.req or DataTransfer).
A00.FR.006	When a Central System communicates with Charge Points with different security profiles or different versions of OCPP.	The Central System MAY operate the Charge Points via different addresses or ports of the Central System. For instance, the Central System server may have one TCP port for TLS with Basic Authentication, and another port for TLS with Client Side Certificates. In this case there is only one security profile in use per port of the Central System, which is allowed.

NOTE Only securing the OCPP communication is not enough to build a secure Charge Point. All other interfaces to the Charge Point should be equally well secured.

2.3. Unsecured Transport with Basic Authentication Profile - 1

Table 4. Security Profile 1 - Unsecured Transport with Basic Authentication

NO.	TYPE	DESCRIPTION
1	**Name**	Unsecured Transport with Basic Authentication
2	**Profile No.**	1
3	**Description**	The Unsecured Transport with Basic Authentication profile provides a low level of security. Charge Point authentication is done through a username and password. No measures are included to secure the communication channel.
4	**Charge Point Authentication**	For Charge Point authentication HTTP Basic authentication is used.
5	**Central System Authentication**	In this profile, the Central System does not authenticate itself to the Charge Point. The Charge Point has to trust that the server it connects to is indeed the Central System.
6	**Communication Security**	No communication security measures are included in the profile.

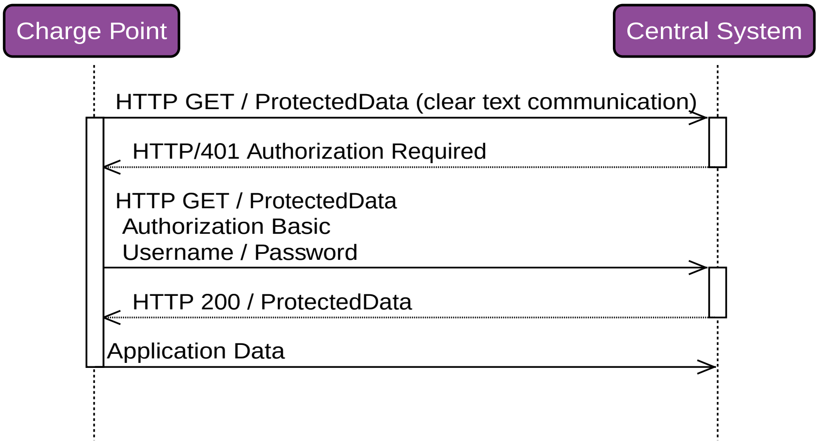

Figure 1. Sequence Diagram: HTTP Basic Authentication sequence diagram

7	**Remark(s)**	The Charge Point should include the same header as used in Basic Auth RFC 2617, while requesting to upgrade the http connection to a websocket connection as described in RFC 6455. The server first needs to validate the Authorization header before upgrading the connection. **Example:** GET /ws HTTP/1.1 Remote-Addr: 127.0.0.1 UPGRADE: websocket CONNECTION: Upgrade HOST: 127.0.0.1:9999 ORIGIN: http://127.0.0.1:9999 SEC-WEBSOCKET-KEY: Pb4obWo2214EfaPQuazMjA== SEC-WEBSOCKET-VERSION: 13 AUTHORIZATION: Basic *<Base64 encoded(<ChargePointId>:<AuthorizationKey>)>*

2.3.1. Unsecured Transport with Basic Authentication Profile - Requirements

Table 5. Security Profile 1 - Unsecured Transport with Basic Authentication - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.201		The Unsecured Transport with Basic Authentication Profile SHOULD only be used in trusted networks.
A00.FR.202		The Charge Point SHALL authenticate itself to the Central System using HTTP Basic authentication [8]
A00.FR.203	A00.FR.202	The client, i.e. the Charge Point, SHALL provide a username and password with every connection request.
A00.FR.204	A00.FR.203	The username SHALL be equal to the Charge Point identity, which is the identifying string of the Charge Point as it uses it in the OCPP-J connection URL.
A00.FR.205	A00.FR.203	The password SHALL be stored in the `AuthorizationKey` Configuration Key. Minimal 16-bytes long, It is strongly advised to be randomly generated binary to get maximal entropy. Hexadecimal represented (20 bytes maximum, represented as a string of up to 40 hexadecimal digits).

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.206	A00.FR.203	With HTTP Basic, the username and password are transmitted in clear text, encoded in base64 only. Hence, it is RECOMMENDED that this mechanism will only be used over connections that are already secured with other means, such as VPNs.

2.4. TLS with Basic Authentication Profile - 2

Table 6. Security Profile 2 - TLS with Basic Authentication

NO.	TYPE	DESCRIPTION
1	**Name**	TLS with Basic Authentication
2	**Profile No.**	2
3	**Description**	In the TLS with Basic Authentication profile, the communication channel is secured using Transport Layer Security (TLS). The Central System authenticates itself using a TLS server certificate. The Charge Points authenticate themselves using HTTP Basic Authentication.
4	**Charge Point Authentication**	For Charge Point authentication HTTP Basic authentication is used. Because TLS is used in this profile, the password will be sent encrypted, reducing the risks of using this authentication method.
5	**Central System Authentication**	The Charge Point authenticates the Central System via the TLS server certificate.
6	**Communication Security**	The communication between Charge Point and Central System is secured using TLS.

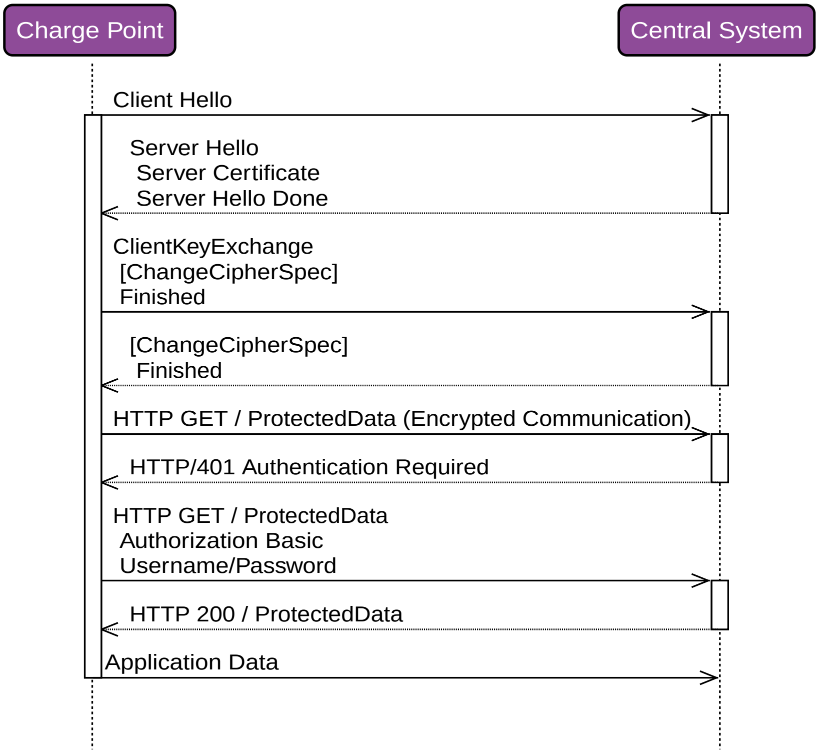

Figure 2. Sequence Diagram: TLS with Basic Authentication sequence diagram

7	**Remark(s)**	TLS allows a number of configurations, not all of which provide sufficient security. The requirements below describe the configurations allowed for OCPP. It is strongly RECOMMENDED to use TLS v1.2 or above for new Charge Points. This also facilitates a later upgrade to OCPP 2.0.1. To provide an adequate level of security for legacy Charge Points that cannot support TLS v1.2 or above, TLS v1.0 or v1.1 MAY be used with cypher suite TLS_RSA_WITH_AES_128_CBC_SHA.

2.4.1. TLS with Basic Authentication Profile - Requirements

Table 7. Security Profile 2 - TLS with Basic Authentication - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.301		The Charge Point SHALL authenticate itself to the Central System using HTTP Basic authentication [8]
A00.FR.302	A00.FR.301	The client, i.e. the Charge Point, SHALL provide a username and password with every connection request.
A00.FR.303	A00.FR.302	The username SHALL be equal to the Charge Point identity, which is the identifying string of the Charge Point as it uses it in the OCPP-J connection URL.
A00.FR.304	A00.FR.302	The password SHALL be stored in the `AuthorizationKey` Configuration Key. Minimal 16-bytes long, It is strongly advised to be randomly generated binary to get maximal entropy. Hexadecimal represented (20 bytes maximum, represented as a string of up to 40 hexadecimal digits).
A00.FR.305		The Central System SHALL act as the TLS server.

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.306		The Central System SHALL authenticate itself by using the Central System certificate as server side certificate.
A00.FR.307		The Charge Point SHALL verify the certification path of the Central System's certificate according to the path validation rules established in Section 6 of [2].
A00.FR.308		The Charge Point SHALL verify that the `commonName` includes the Central System's Fully Qualified Domain Name (FQDN).
A00.FR.309	If the Central System does not own a valid certificate, or if the certification path is invalid	The Charge Point SHALL trigger an InvalidCentralSystemCertificate security event.
A00.FR.310	A00.FR.309	The Charge Point SHALL terminate the connection.
A00.FR.311		The communication channel SHALL be secured using Transport Layer Security (TLS) [3].
A00.FR.312		The Charge Point and Central System SHALL only use TLS v1.2 or above, TLS v1.0/1.1 MAY be used by Charge Points that cannot support TLS v1.2 (NOTE: TLS v1.0/1.1 is not allowed in OCPP 2.0.1).
A00.FR.313		Both of these endpoints SHALL check the version of TLS used.
A00.FR.314	A00.FR.313 AND The Central System detects that the Charge Point only allows connections using an older version of TLS, and TLS v1.0/1.1 not expected for this Charge Point, or only allows SSL	The Central System SHALL terminate the connection.
A00.FR.315	A00.FR.313 AND The Charge Point detects that the Central System only allows connections using an older version of TLS, or only allows SSL	The Charge Point SHALL trigger an InvalidTLSVersion security event AND terminate the connection.
A00.FR.316		TLS SHALL be implemented as in [3] or its successor standards without any modifications.

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.317		The Central System SHALL support at least the following four cipher suites: **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** **TLS_RSA_WITH_AES_128_GCM_SHA256** **TLS_RSA_WITH_AES_256_GCM_SHA384** Note: The Central System will have to provide 2 different certificates to support both Digital Signature Algorithms (RSA and ECDSA). Also when using security profile 3, the Central System should be capable of generating client side certificates for both Digital Signature Algorithms.
A00.FR.318		The Charge Point SHALL support at least the cipher suites: (**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** AND **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**) OR (**TLS_RSA_WITH_AES_128_GCM_SHA256** AND **TLS_RSA_WITH_AES_256_GCM_SHA384**) OR When the Charge Point supports only TLS v1.0/1.1: **TLS_RSA_WITH_AES_128_CBC_SHA** Note: TLS_RSA does not support forward secrecy, therefore TLS_ECDHE is RECOMMENDED. Furthermore, if the Charge Point detects an algorithm used that is not secure, it SHOULD trigger an InvalidTLSCipherSuite security event (send to the Central System via a SecurityEventNotification.req).
A00.FR.319		The Charge Point and Central System SHALL NOT use cipher suites that use cryptographic primitives marked as unsuitable for legacy use in [1]. This will mean that when one (or more) of the cipher suites described in this specification becomes marked as unsuitable for legacy use, it SHALL NOT be used anymore.
A00.FR.320		The TLS Server and Client SHALL NOT use TLS compression methods to avoid compression side-channel attacks and to ensure interoperability as described in Section 6 of [4].
A00.FR.321	A00.FR.320 AND The Central System detects that the Charge Point only allows connections using one of these suites	The Central System SHALL terminate the connection.
A00.FR.322	A00.FR.320 AND The Charge Point detects that the Central System only allows connections using one of these suites	The Charge Point SHALL trigger an InvalidTLSCipherSuite security event AND terminate the connection.
A00.FR.323	When the Central System terminates the connection because of a security reason	It is RECOMMENDED to log a security event in the Central System.

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.324	When the Central System expects Charge Points with only TLS v1.0/1.1 support	The Central System SHOULD support the cypher suite: **TLS_RSA_WITH_AES_128_CBC_SHA** only for TLS v1.0/1.1 connections.

2.5. TLS with Client Side Certificates Profile - 3

Table 8. Security Profile 3 - TLS with Client Side Certificates

NO.	TYPE	DESCRIPTION
1	**Name**	TLS with Client Side Certificates
2	**Profile No.**	3
3	**Description**	In the TLS with Client Side Certificates profile, the communication channel is secured using Transport Layer Security (TLS). Both the Charge Point and Central System authenticate themselves using certificates.
4	**Charge Point Authentication**	The Central System authenticates the Charge Point via the TLS client certificate.
5	**Central System Authentication**	The Charge Point authenticates the Central System via the TLS server certificate.
6	**Communication Security**	The communication between Charge Point and Central System is secured using TLS.

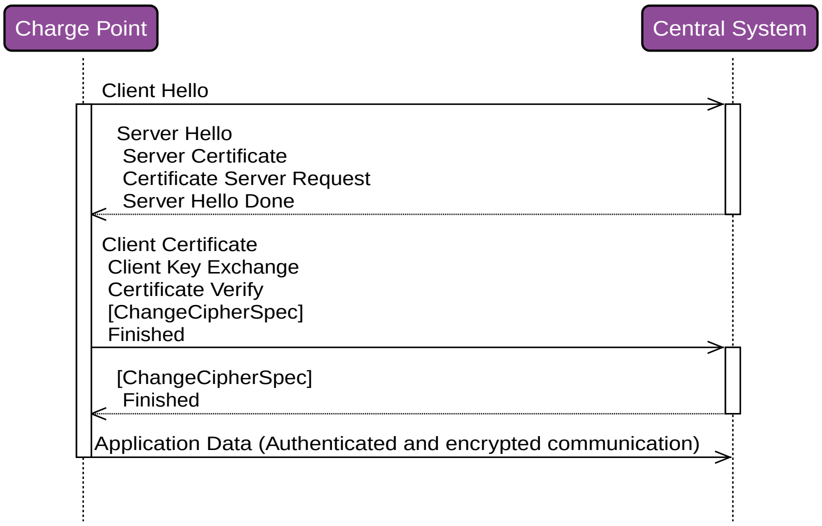

Figure 3. Sequence Diagram: TLS with Client Side Certificates

7	**Remark(s)**	It is strongly RECOMMENDED to use TLS v1.2 or above for new Charge Points. This also facilitates a later upgrade to OCPP 2.0.1. To provide an adequate level of security for legacy Charge Points that cannot support TLS v1.2 or above, TLS v1.0 or v1.1 MAY be used with cypher suite TLS_RSA_WITH_AES_128_CBC_SHA.

2.5.1. TLS with Client Side Certificates Profile - Requirements

Table 9. Security Profile 3 - TLS with Client Side Certificates - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.401		The Charge Point SHALL authenticate itself to the Central System using the Charge Point certificate.
A00.FR.402		The Charge Point certificate SHALL be used as a TLS client side certificate
A00.FR.403		The Central System SHALL verify the certification path of the Charge Point's certificate according to the path validation rules established in Section 6 of [2]
A00.FR.404		The Central System SHALL verify that the certificate is owned by the CPO (or an organization trusted by the CPO) by checking that the O (`organizationName`) RDN in the subject field of the certificate contains the CPO name.
A00.FR.405		The Central System SHALL verify that the certificate belongs to this Charge Point by checking that the CN (`commonName`) RDN in the subject field of the certificate contains the unique Serial Number of the Charge Point
A00.FR.406	If the Charge Point certificate is not owned by the CPO, for instance immediately after installation	it is RECOMMENDED to update the certificate before continuing communication with the Charge Point (also see Installation during manufacturing or installation.)
A00.FR.407	If the Charge Point does not own a valid certificate, or if the certification path is invalid	The Central System SHALL terminate the connection.
A00.FR.408	A00.FR.407	It is RECOMMENDED to log a security event in the Central System.
A00.FR.409		The Central System SHALL act as the TLS server.
A00.FR.410		The Central System SHALL authenticate itself by using the Central System certificate as server side certificate.
A00.FR.411		The Charge Point SHALL verify the certification path of the Central System's certificate according to the path validation rules established in Section 6 of [2].
A00.FR.412		The Charge Point SHALL verify that the `commonName` matches the Central System's Fully Qualified Domain Name (FQDN).
A00.FR.413	If the Central System does not own a valid certificate, or if the certification path is invalid	The Charge Point SHALL trigger an InvalidCentralSystemCertificate security event.
A00.FR.414	A00.FR.413	The Charge Point SHALL terminate the connection.

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.415		The communication channel SHALL be secured using Transport Layer Security (TLS) [3].
A00.FR.416		The Charge Point and Central System SHALL only use TLS v1.2 or above, TLS v1.0/1.1 MAY be used by Charge Points that cannot support TLS v1.2 (NOTE: TLS v1.0/1.1 is not allowed in OCPP 2.0.1).
A00.FR.417		Both of these endpoints SHALL check the version of TLS used.
A00.FR.418	A00.FR.417 AND The Central System detects that the Charge Point only allows connections using an older version of TLS, and TLS v1.0/1.1 not expected for this Charge Point, or only allows SSL	The Central System SHALL terminate the connection.
A00.FR.419	A00.FR.417 AND The Charge Point detects that the Central System only allows connections using an older version of TLS, or only allows SSL	The Charge Point SHALL trigger an InvalidTLSVersion security event AND terminate the connection.
A00.FR.420		TLS SHALL be implemented as in [3] or its successor standards without any modifications.
A00.FR.421		The Central System SHALL support at least the following four cipher suites: **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** **TLS_RSA_WITH_AES_128_GCM_SHA256** **TLS_RSA_WITH_AES_256_GCM_SHA384**
A00.FR.422		The Charge Point SHALL support at least the cipher suites: (**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** AND **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**) OR (**TLS_RSA_WITH_AES_128_GCM_SHA256** AND **TLS_RSA_WITH_AES_256_GCM_SHA384**) OR When the Charge Point supports only TLS v1.0/1.1: **TLS_RSA_WITH_AES_128_CBC_SHA** Note: TLS_RSA does not support forward secrecy, therefore TLS_ECDHE is preferred. Furthermore, if the Charge Point detects an algorithm used that is not secure, it SHOULD trigger an InvalidTLSCipherSuite security event.

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.423		The Charge Point and Central System SHALL NOT use cipher suites that use cryptographic primitives marked as unsuitable for legacy use in [1]. This will mean that when one (or more) of the cipher suites described in this specification becomes marked as unsuitable for legacy use, it SHALL NOT be used anymore.
A00.FR.424		The TLS Server and Client SHALL NOT use TLS compression methods to avoid compression side-channel attacks and to ensure interoperability as described in Section 6 of [4].
A00.FR.425	A00.FR.424 AND If the Central System detects that the Charge Point only allows connections using one of these suites	The Central System SHALL terminate the connection.
A00.FR.426	A00.FR.424 AND The Charge Point detects that the Central System only allows connections using one of these suites	The Charge Point SHALL trigger an InvalidTLSCipherSuite security event AND terminate the connection.
A00.FR.427		A unique Charge Point certificate SHALL be used for each Charge Point.
A00.FR.428	When the Central System expects Charge Points with only TLS v1.0/1.1 support	The Central System SHOULD support the cypher suite: **TLS_RSA_WITH_AES_128_CBC_SHA** only for TLS v1.0/1.1 connections.
A00.FR.429	When Charge Point supports Security Profile 3	The manufacturer is required to give every Charge Point a unique Serial Number.

2.6. Keys used in OCPP

OCPP uses a number of public private key pairs for its security, see below Table. To manage the keys on the Charge Point, messages have been added to OCPP. Updating keys on the Central System or at the manufacturer is out of scope for OCPP. If TLS with Client Side certificates is used, the Charge Point requires a "Charge Point certificate" for authentication against the Central System.

Table 10. Certificates used in the OCPP security specification

CERTIFICATE	PRIVATE KEY STORED AT	DESCRIPTION
Central System Certificate	Central System	Key used to authenticate the Central System.
Central System Root Certificate	Central System	Certificate used to authenticate the Central System.
Charge Point Certificate	Charge Point	Key used to authenticate the Charge Point.

CERTIFICATE	PRIVATE KEY STORED AT	DESCRIPTION
Firmware Signing Certificate	Manufacturer	Key used to verify the firmware signature.
Manufacturer Root Certificate	Manufacturer	Root certificate for verification of the Manufacturer certificate.

2.6.1. Certificate Properties

Table 11. Certificate Properties requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.501		All certificates SHALL use a private key that provides security equivalent to a symmetric key of at least 112 bits according to Section 5.6.1 of [7]. This is the key size that NIST recommends for the period 2011-2030.
A00.FR.502	A00.FR.501 AND RSA or DSA	This translates into a key that SHALL be at least 2048 bits long.
A00.FR.503	A00.FR.501 AND elliptic curve cryptography	This translates into a key that SHALL be at least 224 bits long.
A00.FR.504		For all cryptographic operations, only the algorithms recommended by BSI in [5], which are suitable for use in future systems, SHALL be used. This restriction includes the signing of certificates in the certificate hierarchy
A00.FR.505		For signing by the certificate authority RSA-PSS, or ECDSA SHOULD be used.
A00.FR.506		For computing hash values the SHA256 algorithm SHOULD be used.
A00.FR.507		The certificates SHALL be stored and transmitted in the X.509 format encoded in Privacy-Enhanced Mail (PEM) format.
A00.FR.508		All certificates SHALL include a serial number.
A00.FR.509		The subject field of the certificate SHALL contain the organization name of the certificate owner in the O (`organizationName`) RDN.
A00.FR.510		For the Central System certificate, the subject field SHALL contain the Fully Qualified Domain Name (FQDN) of the server in the CN (`commonName`) RDN

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.511		For the Charge Point certificate, the subject field SHALL contain a CN (`commonName`) RDN which consists of the unique serial number of the Charge Point. This serial number SHALL NOT be in the format of a URL or an IP address so that Charge Point certificates can be differentiated from Central System certificates. Note: According to RFC 2818 [12], if a `subjectAltName` extension of type `dnsName` is present, that must be used as the identity. This would be incompliant with OCPP. Therefore it SHOULD NOT be used in Charge Point and Central System certificates. It is allowed to use the subjectAltName extension of type dnsName for a Central System, when the Central System has multiple network paths to reached it. (for example, via a private APN + VPN using its IP address in the VPN and via public Internet using a named URL)
A00.FR.512		For all certificates the X.509 Key Usage extension [9] SHOULD be used to restrict the usage of the certificate to the operations for which it will be used.

2.6.2. Certificate Hierarchy

This White Paper adds support for the use of two separate certificate hierarchies:

1. The Charge Point Operator hierarchy which contains the Central System, and Charge Point certificates.
2. The Manufacturer hierarchy which contains the Firmware Signing certificate.

The Central System can update the CPO root certificates stored on the Charge Point using the InstallCertificate.req message.

Table 12. Certificate Hierarchy requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.601		The Charge Point Operator MAY act as a certificate authority for the Charge Point Operator hierarchy
A00.FR.602		The private keys belonging to the CPO root certificates MUST be well protected.
A00.FR.603		As the Manufacturer is usually a separate organization from the Charge Point Operator, a trusted third party SHOULD be used as a certificate authority. This is essential to have non-repudiation of firmware images.

2.6.3. Certificate Revocation

In some cases a certificate may become invalid prior to the expiration of the validity period. Such cases include changes of the organization name, or the compromise or suspected compromise of the certificate’s private key. In such cases, the certificate needs to be revoked or indicate it is no longer valid. The revocation of the certificate does not mean that the connection needs to be closed as the the connection can stay open longer than 24 hours.

Different methods are recommended for certificate revocation, see below Table.

Table 13. Recommended revocation methods for the different certificates.

CERTIFICATE	REVOCATION
Central System certificate	Fast expiration
Charge Point certificate	Online verification
Firmware Signing certificate	Online verification

Table 14. Certificate Revocation requirements

ID	PRECOND ITION	REQUIREMENT DEFINITION
A00.FR.701		Fast expiration SHOULD be used to revoke the Central System certificate. (See Note 1)
A00.FR.702		The Central System SHOULD use online certificate verification to verify the validity of the Charge Point certificates.
A00.FR.703		It is RECOMMENDED that a separate certificate authority server is used to manage the certificates.
A00.FR.704		The Central System SHALL verify the validity of the certificate with the certificate authority server. (See Note 2)
A00.FR.706		Prior to providing the certificate for firmware validation to the Charge Point, the Central System SHOULD validate both, the certificate and the signed firmware update.

Note 1: With fast expiration, the certificate is only valid for a short period, less than 24 hours. After that the server needs to request a new certificate from the Certificate Authority, which may be the CPO itself (see section Certificate Hierarchy). This prevents the Charge Points from needing to implement revocation lists or online certificate verification. This simplifies the implementation of certificate management at the Charge Point and reduces communication costs at the Charge Point side. By requiring fast expiration, if the certificate is compromised, the impact is reduced to only a short period.

When the certificate chain should becomes compromised, attackers could used forged certificates to trick a Charge Point to connect to a "fake" Central System. By using fast expiration, the time a Charge Point is vulnerable is greatly reduced.

The Charge Point always communicates with the Certificate Authority through the Central System, this way, if the Charge Points is compromised, the Charge Point cannot attack the CA directly.

Note 2: This allows for immediate revocation of Charge Point certificates. Revocation of Charge Point certificates will happen for instance when a Charge Point is removed. This is more common than revoking the Central System certificate, which is normally only done when it is compromised.

Note 3: It is best practice for any certificate authority server to keep track of revoked certificates.

2.6.4. Installation during manufacturing or installation.

Unique credentials should be used to authenticate each Charge Point to the Central System, whether they are the password used for HTTP Basic Authentication (see Charge Point Authentication) or the Charge Point certificate. These unique credentials have to be put on the Charge Point at some point during manufacturing or installation.

Table 15. Certificate Installation requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A00.FR.801		It is RECOMMENDED that the manufacturer initializes the Charge Point with unique credentials during manufacturing.
A00.FR.802	A00.FR.801	The credentials SHOULD be generated using a cryptographic random number generator, and installed in a secure environment.
A00.FR.803	A00.FR.801	The information needed by the CPO to validate the Charge Point credentials SHOULD be sent to the CPO over a secure channel, so that the CPO can import them in the Central System. For example the password. The Certificate Private key is not needed by the CPO and SHOULD NOT be provided to the CPO.
A00.FR.804	If Charge Point certificates are used.	The manufacturer MAY sign these using their own certificate.
A00.FR.805	A00.FR.804	It is RECOMMENDED that the CPO immediately updates the credentials after installation using the methods described in Section A01 - Update Charge Point Password for HTTP Basic Authentication or A02 - Update Charge Point Certificate by request of the Central System.
A00.FR.806	Before the 'factory credentials' have been updated	The Central System MAY restrict the functionality that the Charge Point can use. The Central System can use the BootNotification state: Pending for this. During the Pending state, the Central System can update the credentials.

A01 - Update Charge Point Password for HTTP Basic Authentication

Table 16. A01 - Password Management

NO.	TYPE	DESCRIPTION
1	**Name**	Update Charge Point Password for HTTP Basic Authentication
2	**ID**	A01 *(OCPP 2.0.1)*
3	**Objective(s)**	This use case defines how to use the authorizationKey, the password used to authenticate Charge Points in the Basic and TLS with Basic Authentication security profiles.
4	**Description**	To enable the Central System to configure a new password for HTTP Basic Authentication, the Central System can send a new value for the `AuthorizationKey` Configuration Key.

NO.	TYPE	DESCRIPTION
	Actors	Charge Point, Central System
	Scenario description	**1.** The Central System sends a ChangeConfiguration.req(key = AuthorizationKey) to the Charge Point with the `AuthorizationKey` Configuration Key. **2.** The Charge Point responds with ChangeConfiguration.conf and the status *Accepted*. **3.** The Charge Point disconnects it current connection. (Storing any queued messages) **4.** The Charge Point connects to the Central System with the new password.
5	**Prerequisite(s)**	Security Profile: Basic Security Profile or TLS with Basic Authentication in use.
6	**Postcondition(s)**	**Successful postcondition:** The Charge Point has reconnected to the Central System with the new password. **Failure postcondition:** If the Charge Point responds to the ChangeConfiguration.req with a ChangeConfiguration.req with a status other than *Accepted*, the Charge Point will keep using the old credentials. The Central System might treat the Charge Point differently, e.g. by not accepting the Charge Point's boot notifications.

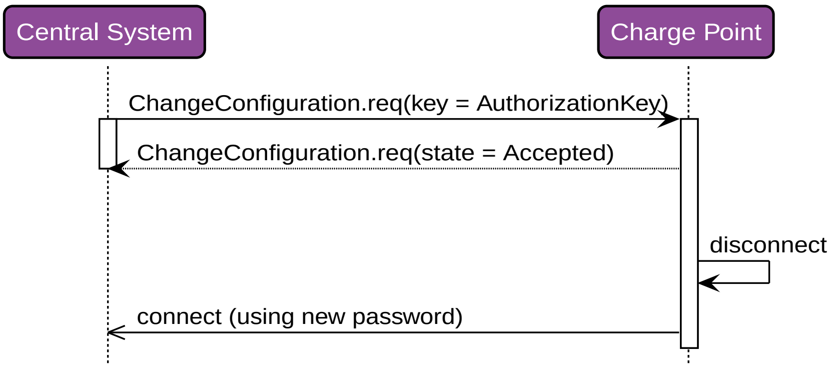
Central System
Charge Point
ChangeConfiguration.req(key = AuthorizationKey)
ChangeConfiguration.req(state = Accepted)
disconnect
connect (using new password)

Figure 4. Update Charge Point Password for HTTP Basic Authentication (happy flow)

7	**Error handling**	n/a
8	**Remark(s)**	n/a

A01 - Update Charge Point Password for HTTP Basic Authentication - Requirements

Table 17. A01 - Update Charge Point Password for HTTP Basic Authentication - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A01.FR.01		The Charge Point SHALL store the password in the configuration key `AuthorizationKey`.

ID	PRECONDITION	REQUIREMENT DEFINITION
A01.FR.02		To set a Charge Point's authorization key via OCPP, the Central System SHALL send the Charge Point a ChangeConfiguration.req message with the `AuthorizationKey` Configuration Key.
A01.FR.03	A01.FR.02 AND The Charge Point responds to this ChangeConfiguration.req with a ChangeConfiguration.conf with status *Accepted*.	The Central System SHALL assume that the authorization key change was successful, and no longer accept the credentials previously used by the Charge Point.
A01.FR.04	A01.FR.02 AND The Charge Point responds to this ChangeConfiguration.req with a ChangeConfiguration.conf with status *Rejected* or *NotSupported*.	The Central System SHALL assume that the Charge Point has NOT changed the password. Therefore the Central System SHALL keep accepting the old credentials.
A01.FR.05	A01.FR.04	While the Central System SHALL still accepts a connection from the Charge Point, it MAY restrict the functionality that the Charge Point can use. The Central System can use the BootNotification state: Pending for this. During the Pending state, the Central System can for example retry to update the credentials.
A01.FR.06		Different passwords SHOULD be used for different Charge Points.
A01.FR.07		Passwords SHOULD be generated randomly to ensure that the passwords have sufficient entropy.
A01.FR.08		the Central System SHOULD only store salted password hashes, not the passwords themselves.
A01.FR.09		the Central System SHOULD NOT put the passwords in clear-text in log files or debug information. In this way, if the Central System is compromised not all Charge Point password will be immediately compromised.
A01.FR.10		On the Charge Point the password needs to be stored in clear-text. Extra care SHOULD be taken into storing it securely. Definitions of mechanisms how to securely store the credentials are however not in scope of the OCPP Security Profiles.
A01.FR.11	A01.FR.02	The Charge Point SHALL log the change of `AuthorizationKey` in the Security log.
A01.FR.12	A01.FR.11	The Charge Point SHALL NOT disclose the content of the `AuthorizationKey` in its logging. This is to prevent exposure of key material to persons that may have access to a diagnostics file.

A02 - Update Charge Point Certificate by request of Central System

Table 18. A02 - Update Charge Point Certificate by request of Central System

NO.	TYPE	DESCRIPTION
1	**Name**	Update Charge Point Certificate by request of Central System
2	**ID**	A02 *(OCPP 2.0.1)*
3	**Objective(s)**	To facilitate the management of the Charge Point client side certificate, a certificate update procedure is provided.
4	**Description**	The Central System requests the Charge Point to update its key using ExtendedTriggerMessage.req (SignChargePointCertificate).
	Actors	Charge Point, Central System, Certificate Authority Server
	Scenario description	**1.** The Central System requests the Charge Point to update its certificate using the ExtendedTriggerMessage.req (SignChargePointCertificate) message. **2.** The Charge Point responds with ExtendedTriggerMessage.conf **3.** The Charge Point generates a new public / private key pair. **4.** The Charge Point sends a SignCertificate.req to the Central System. **5.** The Central System responds with SignCertificate.conf, with status *Accepted*. **6.** The Central System forwards the CSR to the Certificate Authority Server. **7.** Certificate Authority Server signs the certificate. **8.** The Certificate Authority Server returns the Signed Certificate to the Central System. **9.** The Central System sends CertificateSigned.req to the Charge Point. **10.** The Charge Point verifies the Signed Certificate. **11.** The Charge Point responds with h to the Central System with the status *Accepted* or *Rejected*.
5	**Prerequisite(s)**	The configuration variable `CpoName` MUST be set.
6	**Postcondition(s)**	**Successful postcondition:** New Client Side certificate installed in the Charge Point. **Failure postcondition:** New Client Side certificate is rejected and discarded.

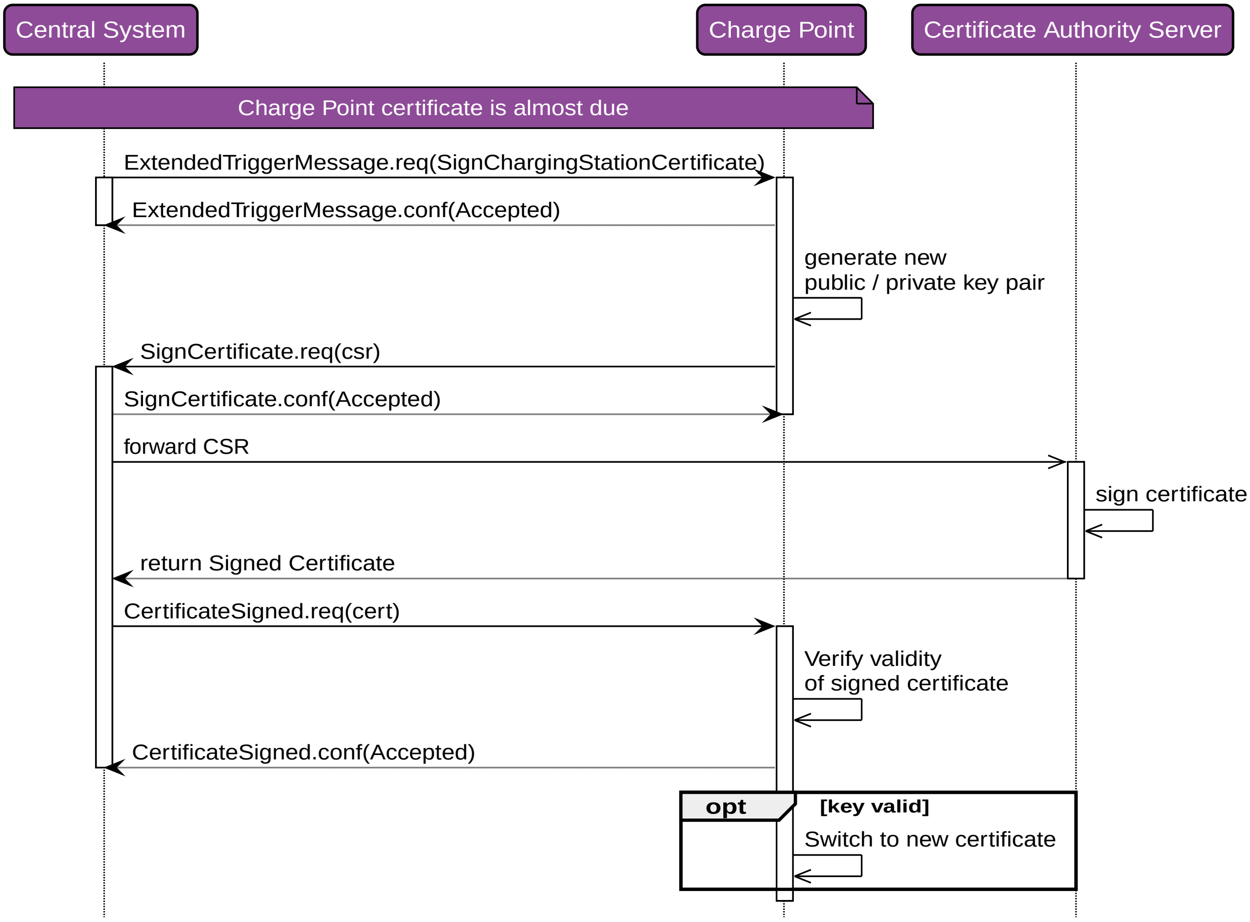
Central System
Charge Point
Certificate Authority Server
Charge Point certificate is almost due
ExtendedTriggerMessage.req(SignChargingStationCertificate)
ExtendedTriggerMessage.conf(Accepted)
generate new
public / private key pair
SignCertificate.req(csr)
SignCertificate.conf(Accepted)
forward CSR
sign certificate
return Signed Certificate
CertificateSigned.req(cert)
Verify validity
of signed certificate
CertificateSigned.conf(Accepted)
opt
[key valid]
Switch to new certificate

Figure 5. Update Charge Point Certificate

7	**Error handling**	The Central System accepts the CSR request from the Charge Point, before forwarding it to the CA. But when the CA cannot be reached, or rejects the CSR, the Charge Point will never known. The Central System may do some checks on the CSR, but cannot do all the checks that a CA does, and it does not prevent connection timeout to the CA. When something like this goes wrong, either the CA is offline or the CSR send by the Charge Point is not correct, according to the CA. In both cases this is something an operator at the CPO needs to be notified of. The operator then needs to investigate the issue. When resolved, the operator can re-run A02. It is NOT RECOMMENDED to let the Charge Point retry when the certificate is not send within X minutes or hours. When the CSR is incorrect, that will not be resolved automatically. It is possible that only a new firmware will fix this.
8	**Remark(s)**	The CPO may act as a Certification Authority, so the CA Server may be a local server. The applicable Certification Authority SHALL check the information in the CSR. If it is correct, the Certificate Authority SHALL sign the CSR, send it to the CPO, the CPO sends it back to the Charge Point in the CertificateSigned.req message The certificate authority SHOULD implement strong measures to keep the certificate signing private keys secure. Even though the messages CertificateSigned.req (see use cases A02 and A03) and InstallCertificate.req (use case M05 - Install CA Certificate in a Charge Point) are both used to send certificates, their purposes are different. CertificateSigned.req is used to return the the Charge Points *own* public certificate signed by a Certificate Authority. InstallCertificate.req is used to install Root certificates. For (Sub-)CA certificate handling see use cases M03 - Retrieve list of available certificates from a Charge Point, M04 - Delete a specific certificate from a Charge Point, M05 - Install CA certificate in a Charge Point.

A02 - Update Charge Point Certificate by request of Central System - Requirements

Table 19. A02 - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A02.FR.01		A key update SHOULD be performed after installation of the Charge Point, to change the key from the one initially provisioned by the manufacturer (possibly a default key).
A02.FR.02	After sending a ExtendedTriggerMessage.conf.	The Charge Point SHALL generate a new public / private key pair using one of the key generation functions described in Section 4.2.1.3 of [6].
A02.FR.03	A02.FR.02	The Charge Point SHALL send the public key in form of a Certificate Signing Request (CSR) as described in RFC 2986 [14] and then PEM encoded, using the SignCertificate.req message.
A02.FR.04		The Central System SHOULD NOT sign the certificate itself, but instead forwards the CSR to a dedicated certificate authority server managing the certificates for the Charge Point infrastructure. The dedicated authority server MAY be operated by the CPO.
A02.FR.05		The private key generated by the Charge Point during the key update process SHALL NOT leave the Charge Point at any time, and SHALL NOT be readable via OCPP or any other (remote) communication connection.
A02.FR.06		The Charge Point SHALL verify the validity of the signed certificate in the CertificateSigned.req message, checking at least the period when the certificate is valid, the properties in Certificate Properties, and that it is part of the Charge Point Operator certificate hierarchy as described in Certificate Hierarchy.
A02.FR.07	If the certificate is not valid.	The Charge Point SHALL discard the certificate, and trigger an InvalidChargePointCertificate security event.
A02.FR.08		The Charge Point SHALL switch to the new certificate as soon as the current date and time is after the ‘Not valid before’ field in the certificate.
A02.FR.09	If the Charge Point contains more than one valid certificate of the same type.	The Charge Point SHALL use the newest certificate, as measured by the start of the validity period.
A02.FR.10	When the Charge Point has validated that the new certificate works	The Charge Point MAY discard the old certificate. It is RECOMMENDED to store old certificates for one month, as fallback.
A02.FR.11	Upon receipt of a SignCertificate.req AND It is able to process the request	The Central System SHALL set status to *Accepted* in the SignCertificate.conf.

ID	PRECONDITION	REQUIREMENT DEFINITION
A02.FR.12	Upon receipt of a SignCertificate.req AND It is NOT able to process the request	The Central System SHALL set status to *Rejected* in the SignCertificate.conf.
A02.FR.13	A02.FR.03	The Charge Point SHALL put the value of the `CpoName` configuration key in the organizationName (O) RDN in the CSR subject field.

A03 - Update Charge Point Certificate initiated by the Charge Point

Table 20. A03 - Update Charge Point Certificate initiated by the Charge Point

NO.	TYPE	DESCRIPTION
1	**Name**	Update Charge Point Certificate initiated by the Charge Point
2	**ID**	A03 *(OCPP 2.0.1)*
3	**Objective(s)**	To facilitate the management of the Charge Point client side certificate, a certificate update procedure is provided.
4	**Description**	The Charge Point detects that the 'Charge Point Certificate' it is using will expire in one month. The Charge Point initiates the process to update its key using SignCertificate.req.
	Actors	Charge Point, Central System, Certificate Authority Server
	Scenario description	**1.** The Charge Point detects that the Charge Point certificate is due to expire. **2.** The Charge Point generates a new public / private key pair. **3.** The Charge Point sends a SignCertificate.req to the Central System. **4.** The Central System responds with a SignCertificate.conf, with status *Accepted*. **5.** The Central System forwards the CSR to the Certificate Authority Server. **6.** Certificate Authority Server signs the certificate. **7.** The Certificate Authority Server returns the Signed Certificate to the Central System. **8.** The Central System sends a CertificateSigned.req to the Charge Point. **9.** The Charge Point verifies the Signed Certificate. **10.** The Charge Point responds with a CertificateSigned.conf to the Central System with the status *Accepted* or *Rejected*.
5	**Prerequisite(s)**	The configuration variable `CpoName` MUST be set.
6	**Postcondition(s)**	**Successful postcondition:** New Client Side certificate installed in the Charge Point. **Failure postcondition:** New Client Side certificate is rejected and discarded.

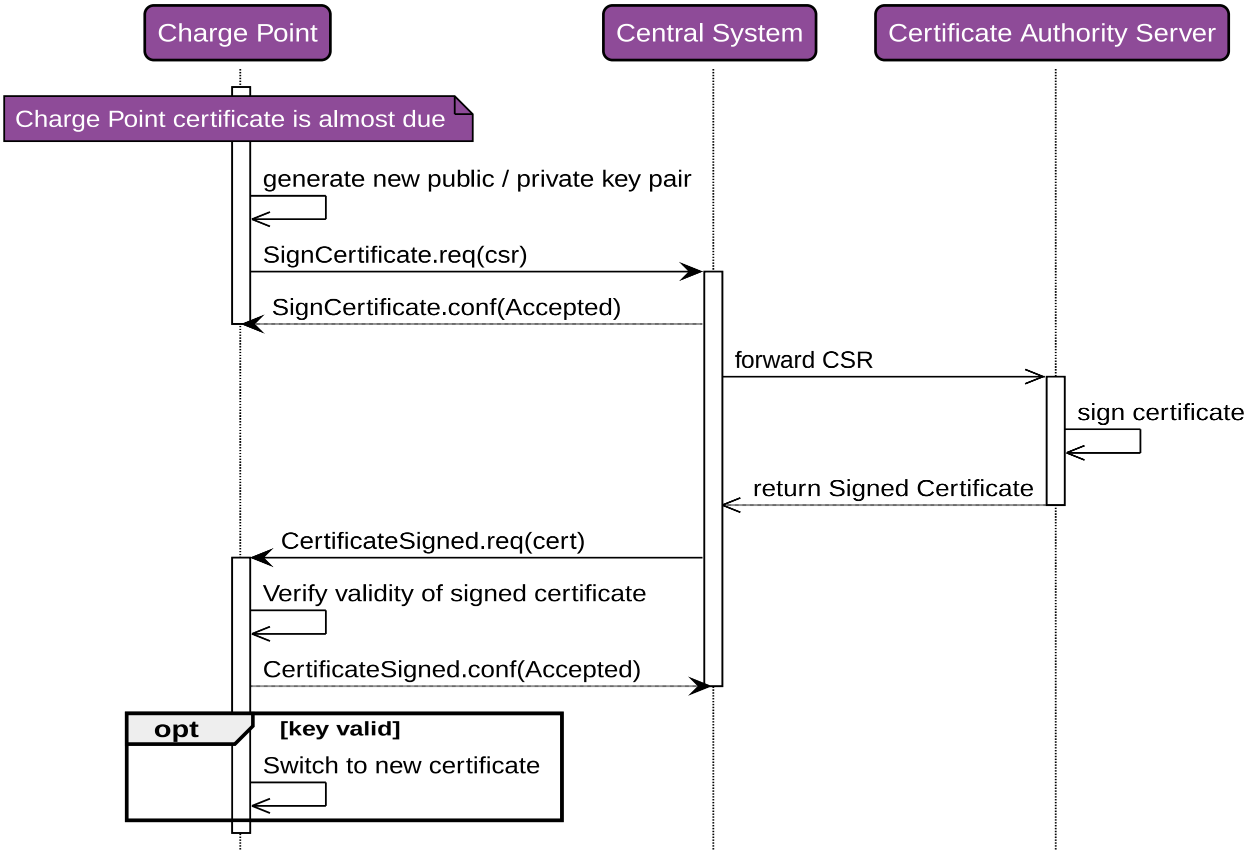
Charge Point
Central System
Certificate Authority Server
Charge Point certificate is almost due
generate new public / private key pair
SignCertificate.req(csr)
SignCertificate.conf(Accepted)
forward CSR
sign certificate
return Signed Certificate
CertificateSigned.req(cert)
Verify validity of signed certificate
CertificateSigned.conf(Accepted)
opt
[key valid]
Switch to new certificate

Figure 6. Update Charge Point Certificate initiated by Charge Point

7	**Error handling**	The Central System accepts the CSR request from the Charge Point, before forwarding it to the CA. But when the CA cannot be reached, or rejects the CSR, the Charge Point will never known. The Central System may do some checks on the CSR, but cannot do all the checks that a CA does, and it does not prevent connection timeout to the CA. When something like this goes wrong, either the CA is offline or the CSR send by the Charge Point is not correct, according to the CA. In both cases this is something an operator at the CPO needs to be notified of. The operator then needs to investigate the issue. When resolved, the operator can re-run A02. It is NOT RECOMMENDED to let the Charge Point retry when the certificate is not send within X minutes or hours. When the CSR is incorrect, that will not be resolved automatically. It is possible that only a new firmware will fix this.
8	**Remark(s)**	Same remarks as in A02 - Update Charge Point Certificate by request of Central System apply.

A03 - Update Charge Point Certificate initiated by the Charge Point - Requirements

Table 21. A03 - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A03.FR.01		A key update MAY be performed after installation of the Charge Point, to change the key from the one initially provisioned by the manufacturer (possibly a default key).
A03.FR.02	When the Charge Point detects that the current Charge Point certificate will expire in one month.	The Charge Point SHALL generate a new public / private key pair using one of the key generation functions described in Section 4.2.1.3 of [6].

ID	PRECONDITION	REQUIREMENT DEFINITION
A03.FR.03	A03.FR.02	The Charge Point SHALL send the public key in form of a Certificate Signing Request (CSR) as described in RFC 2986 [14] and then PEM encoded, using the SignCertificate.req message.
A03.FR.04		The Central System SHOULD NOT sign the certificate itself, but instead forwards the CSR to a dedicated certificate authority server managing the certificates for the Charge Point infrastructure. The dedicated authority server MAY be operated by the CPO.
A03.FR.05		The private key generated by the Charge Point during the key update process SHALL NOT leave the Charge Point at any time, and SHALL NOT be readable via OCPP or any other (remote) communication connection.
A03.FR.06		The Charge Point SHALL verify the validity of the signed certificate in the CertificateSigned.req message, checking at least the period when the certificate is valid, the properties in Certificate Properties, and that it is part of the Charge Point Operator certificate hierarchy as described in Certificate Hierarchy.
A03.FR.07	If the certificate is not valid.	The Charge Point SHALL discard the certificate, and trigger an InvalidChargePointCertificate security event.
A03.FR.08		The Charge Point SHALL switch to the new certificate as soon as the current date and time is after the ‘Not valid before’ field in the certificate.
A03.FR.09	If the Charge Point contains more than one valid certificate of the same type.	The Charge Point SHALL use the newest certificate, as measured by the start of the validity period.
A03.FR.10	When the Charge Point has validated that the new certificate works	The Charge Point MAY discard the old certificate. It is RECOMMENDED to store old certificates for one month, as fallback.
A03.FR.11	Upon receipt of a SignCertificate.req AND It is able to process the request	The Central System SHALL set status to *Accepted* in the SignCertificate.conf.
A03.FR.12	Upon receipt of a SignCertificate.req AND It is NOT able to process the request	The Central System SHALL set status to *Rejected* in the SignCertificate.conf.
A03.FR.13	A03.FR.03	The Charge Point SHALL put the value of `CpoName` in the organizationName RDN in the CSR subject field.

A05 - Upgrade Charge Point Security Profile

Table 22. A05 - Upgrade Charge Point Security Profile

NO.	TYPE	DESCRIPTION
1	**Name**	Upgrade Charge Point Security Profile
2	**ID**	A05 *(OCPP 2.0.1)*
3	**Objective(s)**	Upgrade the security profile used by a Charge Point to a higher profile.
4	**Description**	The CPO wants to increase the security of the OCPP connection between Central System and a Charge Point. This use case is especially relevant when migrating from OCPP 1.6 without security profiles to OCPP 1.6 with security profiles, before migrating to a security profile the prerequisites, like installed certificates or password need to be configured. The CPO ensures the prerequisite(s) for going to a higher security certificates are met before sending the command to change to a higher security profile. the Charge Point reconnects to the Central System using the higher security profile.
	Actors	Charge Point, Central System, CPO
	Scenario description	**1.** CPO command the Central System to upgrade a Charge Point to a higher Security Profile. **2.** The Central System sends a ChangeConfiguration.req for configuration key: `SecurityProfile` with a new (higher) value to the Charge Point. **3.** The Charge Point checks all the prerequisites for the new Security Profile. **4.** The Charge Point responds with ChangeConfiguration.conf. **5.** The Charge Point disconnects it's current connection the Central System. **6.** The Charge Point connects to the Central System using the new Security Profile.
5	**Prerequisite(s)**	Configuration Key: `SecurityProfile` available.
6	**Postcondition(s)**	**Successful postcondition:** The Charge Point is using the higher security profile. **Failure postcondition:** The Charge Point is NOT using the higher security profile.

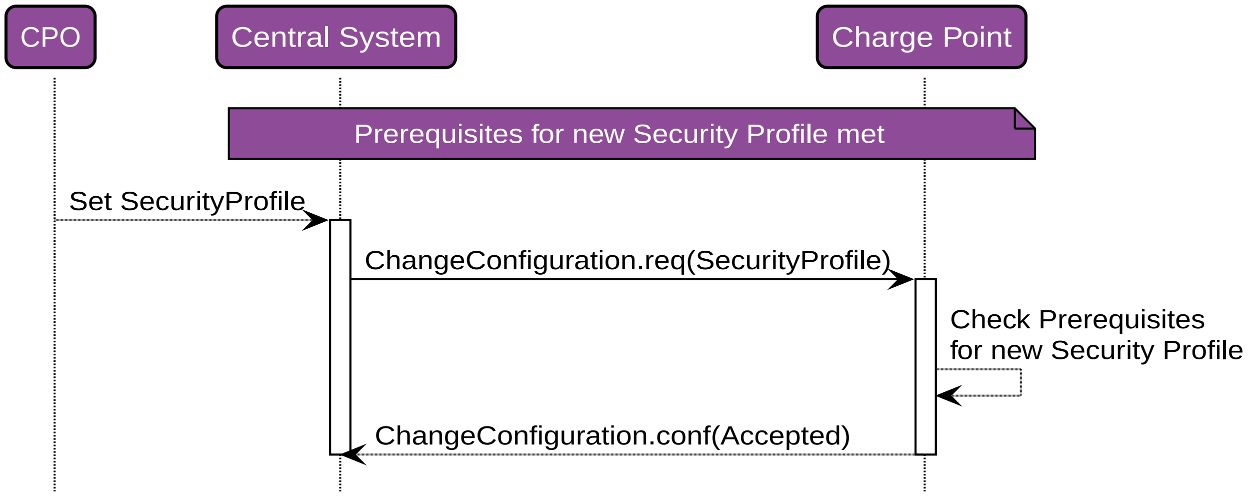
CPO
Central System
Charge Point
Prerequisites for new Security Profile met
Set SecurityProfile
ChangeConfiguration.req(SecurityProfile)
Check Prerequisites
for new Security Profile
ChangeConfiguration.conf(Accepted)

Figure 7. Upgrade Charge Point Certificate initiated by Charge Point

7	**Error handling**	If the Charge Point is unable to connect to the Central System using the configured (higher) security profile, it SHOULD fallback to its previous security profile settings. This is to prevent that the Charge Point will become unable to reconnect to the Central System on its own.
8	**Remark(s)**	For security reasons it is not allowed to change to a lower Security Profile over OCPP.

A05 - Upgrade Charge Point Security Profile - Requirements

Table 23. A05 - Requirements

ID	PRECONDITION	REQUIREMENT DEFINITION
A05.FR.01	Charge Point receives ChangeConfiguration.req for `SecurityProfile` with a value lower or equal to the current value.	The Charge Point SHALL respond with ChangeConfiguration.conf(Rejected), and not change the value for `SecurityProfile` and/or reconnect to the Central System.
A05.FR.02	Charge Point receives ChangeConfiguration.req for `SecurityProfile` with a value higher then the current value AND new value is 1 or 2 AND configuration key: `AuthorizationKey` does not contain a value (that meets the requirements for `AuthorizationKey`)	The Charge Point SHALL respond with ChangeConfiguration.conf(Rejected), and not change the value for `SecurityProfile` and/or reconnect to the Central System.
A05.FR.03	Charge Point receives ChangeConfiguration.req for `SecurityProfile` with a value higher then the current value AND new value is 2 or 3 AND No valid CentralSystemRootCertificate installed	The Charge Point SHALL respond with ChangeConfiguration.conf(Rejected), and not change the value for `SecurityProfile` and/or reconnect to the Central System.
A05.FR.04	Charge Point receives ChangeConfiguration.req for `SecurityProfile` with a value higher then the current value AND new value is 3 AND No valid ChargePointCertificate installed	The Charge Point SHALL respond with ChangeConfiguration.conf(Rejected), and not change the value for `SecurityProfile` and/or reconnect to the Central System.
A05.FR.05	Charge Point receives ChangeConfiguration.req for `SecurityProfile` with a value higher then the current value AND all prerequisites are met	The Charge Point SHALL respond with ChangeConfiguration.conf(Accepted)
A05.FR.06	A05.FR.05	The Charge Point SHALL disconnect from the Central System
A05.FR.07	A05.FR.06	The Charge Point SHALL reconnect the Central System with the new Security Profile
A05.FR.08	A05.FR.07 AND The Charge Point was unable to connect to the Central System	The Charge Point SHOULD fallback to its previous security profile setting.