A. Security

1. OCPP Security

This Functional Block describes the security requirements for the OCPP protocol. The security part 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 [21]. Security requirements are included on security measures at Charging Station and CSMS, to support users of the OCPP.

1.1. 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 CSMS and Charging Station. The integrity and confidentiality of messages on this channel should be protected with strong cryptographic measures.
2. To provide mutual authentication between the Charging Station and the CSMS. Both parties should be able to identify who they are communicating with.
3. To provide a secure firmware update process by allowing the Charging Station 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. A list of security related events and their 'criticality' is provided in the appendices.

1.2. Design Considerations

This section is informative.

The security Functional Block 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 CSMS usually acts as the server, different users or role-based access control on the Charging Station are not implemented in this standard. To mitigate this, it is recommended to implement access control on the CSMS. To make sure the mechanisms implemented there cannot be bypassed, OCPP should not be used by qualified personnel performing maintenance to Charging Stations locally at the Charging Station, as other protocols may be used for local maintenance purposes.

1.3. Security Profiles

This section defines the different OCPP security profiles and their requirement. OCPP 2.0.1 supports three security profiles: The table below shows which security measures are used by which profile.

Table 11. Overview of OCPP security profiles

Profile	Charging Station Authentication	CSMS 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 CSMS, 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 CSMS and the Charging Station. For field operation it is highly recommended to use a security profile with TLS.
- In some cases (e.g. lab installations, test setups, etc.) one might prefer to use OCPP 2.0.1 without implementing security. While this is possible, it is NOT considered a valid OCPP 2.0.1 implementation.

1.3.1. Generic Security Profile requirements

Table 12. Generic Security Profile requirements

ID	Precondition	Requirement definition
A00.FR.001		The Charging Station and CSMS SHALL only use one security profile at a time
A00.FR.002	If the Charging Station tries to connect with a different profile than the CSMS is using	The CSMS SHALL terminate the connection.
A00.FR.003	If the CSMS tries to connect with a different profile than the Charging Station is using	The Charging Station SHALL terminate the connection.
A00.FR.004		The security profile SHALL be configured before OCPP communication is possible.
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. SetVariablesRequest or DataTransferRequest).
A00.FR.006	When a CSMS communicates with Charging Stations with different security profiles or different versions of OCPP.	The CSMS MAY operate the Charging Stations via different addresses or ports of the CSMS. For instance, the CSMS 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 CSMS, which is allowed.

1.3.2. Unsecured Transport with Basic Authentication Profile - 1

Table 13. 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. Charging Station authentication is done through a username and password. No measures are included to secure the communication channel.
4	**Charging Station Authentication**	For Charging Station authentication HTTP Basic authentication is used.

No.	Type	Description
5	**CSMS Authentication**	In this profile, the CSMS does not authenticate itself to the Charging Station. The Charging Station has to trust that the server it connects to is indeed the CSMS.
6	**Communication Security**	No communication security measures are included in the profile.

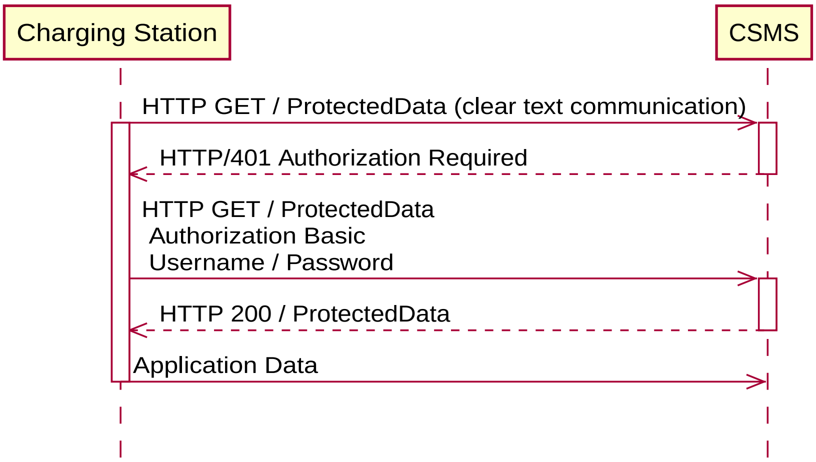

Figure 2. Sequence Diagram: HTTP Basic Authentication sequence diagram

7	**Remark(s)**	n/a

1.3.3. Unsecured Transport with Basic Authentication Profile - Requirements

Table 14. 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 Charging Station SHALL authenticate itself to the CSMS using HTTP Basic authentication [18]
A00.FR.203	A00.FR.202	The client, i.e. the Charging Station, SHALL provide a username and password with every connection request.
A00.FR.204	A00.FR.203	The username SHALL be equal to the Charging Station identity, which is the identifying string of the Charging Station as it uses it in the OCPP-J connection URL. When using Basic Authentication, the Charging Station identity may not contain the character ":". Otherwise the CSMS may be unable to separate the username from the password.
A00.FR.205	A00.FR.203	The password SHALL be stored in the `BasicAuthPassword` Configuration Variable. It SHALL be a randomly chosen identifierString with a sufficiently high entropy, consisting of minimum 16 and maximum 40 characters (alpha-numeric characters and the special characters allowed by identifierString). The password SHALL be sent as a UTF-8 encoded string (NOT encoded into octet string or base64).
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.

1.3.4. TLS with Basic Authentication Profile - 2

Table 15. 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 CSMS authenticates itself using a TLS server certificate. The Charging Stations authenticate themselves using HTTP Basic Authentication.

No.	Type	Description
4	**Charging Station Authentication**	For Charging Station 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	**CSMS Authentication**	The Charging Station authenticates the CSMS via the TLS server certificate.
6	**Communication Security**	The communication between Charging Station and CSMS is secured using TLS.
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. The Charging Station 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>)>*

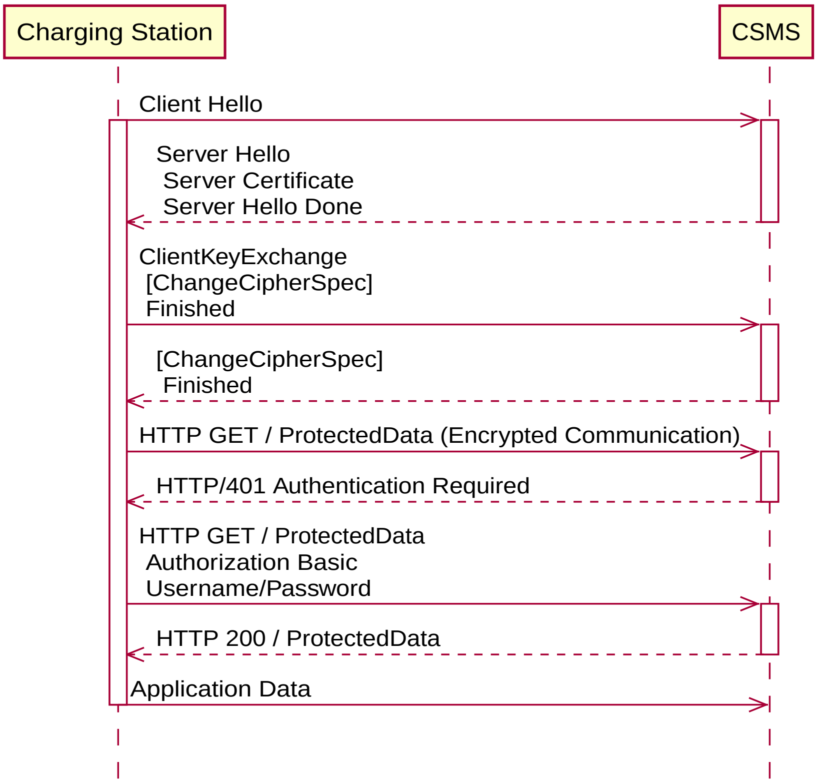

Figure 3. Sequence Diagram: TLS with Basic Authentication sequence diagram

1.3.5. TLS with Basic Authentication Profile - Requirements

Table 16. Security Profile 2 - TLS with Basic Authentication - Requirements

ID	Precondition	Requirement definition
A00.FR.301		The Charging Station SHALL authenticate itself to the CSMS using HTTP Basic authentication [18]

ID	Precondition	Requirement definition
A00.FR.302	A00.FR.301	The client, i.e. the Charging Station, SHALL provide a username and password with every connection request.
A00.FR.303	A00.FR.302	The username SHALL be equal to the Charging Station identity, which is the identifying string of the Charging Station as it uses it in the OCPP-J connection URL. When using Basic Authentication, the Charging Station identity may not contain the character ":". Otherwise the CSMS may be unable to separate the username from the password.
A00.FR.304	A00.FR.302	The password SHALL be stored in the `BasicAuthPassword` Configuration Variable. It SHALL be a randomly chosen identifierString with a sufficiently high entropy, consisting of minimum 16 and maximum 40 characters (alpha-numeric characters and the special characters allowed by identifierString). The password SHALL be sent as a UTF-8 encoded string (NOT encoded into octet string or base64).
A00.FR.306		The CSMS SHALL act as the TLS server.
A00.FR.307		The CSMS SHALL authenticate itself by using the CSMS certificate as server side certificate.
A00.FR.308		The Charging Station SHALL verify the certification path of the CSMS's certificate according to the path validation rules established in Section 6 of [3].
A00.FR.309		The Charging Station SHALL verify that the `commonName` includes the CSMS's FQDN.
A00.FR.310	If the CSMS does not own a valid certificate, or if the certification path is invalid	The Charging Station SHALL trigger an InvalidCsmsCertificate security event (See part 2 appendices for the full list of security events).
A00.FR.311	A00.FR.310	The Charging Station SHALL terminate the connection.
A00.FR.312		The communication channel SHALL be secured using Transport Layer Security (TLS) [4].
A00.FR.313		The Charging Station and CSMS SHALL only use TLS v1.2 or above.
A00.FR.314		Both of these endpoints SHALL check the version of TLS used.
A00.FR.315	A00.FR.314 AND The CSMS detects that the Charging Station only allows connections using an older version of TLS, or only allows SSL	The CSMS SHALL terminate the connection.
A00.FR.316	A00.FR.314 AND The Charging Station detects that the CSMS only allows connections using an older version of TLS, or only allows SSL	The Charging Station SHALL trigger an InvalidTLSVersion security event AND terminate the connection (See part 2 appendices for the full list of security events).
A00.FR.317		TLS SHALL be implemented as in [4] or its successor standards without any modifications.
A00.FR.318		The CSMS 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 CSMS will have to provide 2 different certificates to support both cipher suites. Also when using security profile 3, the CSMS should be capable of generating client side certificates for both cipher suites.

ID	Precondition	Requirement definition
A00.FR.319		The Charging Station 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**) Note 1: TLS_RSA does not support forward secrecy, therefore TLS_ECDHE is RECOMMENDED. Furthermore, if the Charging Station detects an algorithm used that is not secure, it SHOULD trigger an InvalidTLSCipherSuite security event (See part 2 appendices for the full list of security events). Note 2: Please note that ISO15118-2 prescribes to implement the following cipher suites for the communication between EV and Charging Station: TLS_ECDH_ECDSA_WITH_AES_128_**CBC**_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_**CBC**_SHA256
A00.FR.320		The Charging Station and CSMS 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.321		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 [10].
A00.FR.322	A00.FR.321 AND The CSMS detects that the Charging Station only allows connections using one of these suites	The CSMS SHALL terminate the connection.
A00.FR.323	A00.FR.321 AND The Charging Station detects that the CSMS only allows connections using one of these suites	The Charging Station SHALL trigger an InvalidTLSCipherSuite security event AND terminate the connection (See part 2 appendices for the full list of security events).

1.3.6. TLS with Client Side Certificates Profile - 3

Table 17. 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 Charging Station and CSMS authenticate themselves using certificates.
4	**Charging Station Authentication**	The CSMS authenticates the Charging Station via the TLS client certificate.
5	**CSMS Authentication**	The Charging Station authenticates the CSMS via the TLS server certificate.
6	**Communication Security**	The communication between Charging Station and CSMS is secured using TLS.

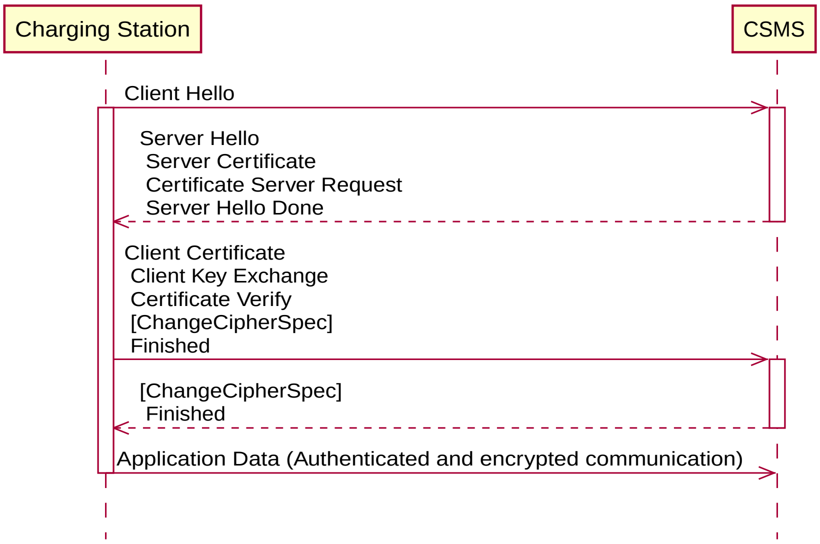

Figure 4. Sequence Diagram: TLS with Client Side Certificates

7	**Remark(s)**	N/a

1.3.7. TLS with Client Side Certificates Profile - Requirements

Table 18. Security Profile 3 - TLS with Client Side Certificates - Requirements

ID	Precondition	Requirement definition
A00.FR.401		The Charging Station SHALL authenticate itself to the CSMS using the Charging Station certificate.
A00.FR.402		The Charging Station certificate SHALL be used as a TLS client side certificate
A00.FR.403		The CSMS SHALL verify the certification path of the Charging Station’s certificate according to the path validation rules established in Section 6 of [3]
A00.FR.404		The CSMS SHALL verify that the certificate is owned by the CSO (or an organization trusted by the CSO) by checking that the O (`organizationName`) RDN in the subject field of the certificate contains the CSO name.
A00.FR.405		The CSMS SHALL verify that the certificate belongs to this Charging Station by checking that the CN (`commonName`) RDN in the subject field of the certificate contains the unique serial number of the Charging Station (see Certificate Properties).
A00.FR.406	If the Charging Station certificate is not owned by the CSO, for instance immediately after installation	it is RECOMMENDED to update the certificate before continuing communication with the Charging Station (also see Installation)
A00.FR.407	If the Charging Station does not own a valid certificate, or if the certification path is invalid	The CSMS SHALL terminate the connection.
A00.FR.408	A00.FR.407	It is RECOMMENDED to log a security event in the CSMS.
A00.FR.409		The CSMS SHALL act as the TLS server.
A00.FR.410		The CSMS SHALL authenticate itself by using the CSMS certificate as server side certificate.
A00.FR.411		The Charging Station SHALL verify the certification path of the CSMS’s certificate according to the path validation rules established in Section 6 of [3].
A00.FR.412		The Charging Station SHALL verify that the `commonName` matches the CSMS’s FQDN.
A00.FR.413	If the CSMS does not own a valid certificate, or if the certification path is invalid	The Charging Station SHALL trigger an InvalidCsmsCertificate security event (See part 2 appendices for the full list of security events).
A00.FR.414	A00.FR.413	The Charging Station SHALL terminate the connection.

ID	Precondition	Requirement definition
A00.FR.415		The communication channel SHALL be secured using Transport Layer Security (TLS) [4].
A00.FR.416		The Charging Station and CSMS SHALL only use TLS v1.2 or above.
A00.FR.417		Both of these endpoints SHALL check the version of TLS used.
A00.FR.418	A00.FR.417 AND The CSMS detects that the Charging Station only allows connections using an older version of TLS, or only allows SSL	The CSMS SHALL terminate the connection.
A00.FR.419	A00.FR.417 AND The Charging Station detects that the CSMS only allows connections using an older version of TLS, or only allows SSL	The Charging Station SHALL trigger an InvalidTLSVersion security event AND terminate the connection (See part 2 appendices for the full list of security events).
A00.FR.420		TLS SHALL be implemented as in [4] or its successor standards without any modifications.
A00.FR.421		The CSMS 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 CSMS will have to provide 2 different certificates to support both cipher suites. Also when using security profile 3, the CSMS should be capable of generating client side certificates for both cipher suites.
A00.FR.422		The Charging Station 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**) Note 1: TLS_RSA does not support forward secrecy, therefore TLS_ECDHE is RECOMMENDED. Furthermore, if the Charging Station detects an algorithm used that is not secure, it SHOULD trigger an InvalidTLSCipherSuite security event (See part 2 appendices for the full list of security events). Note 2: Please note that ISO15118-2 prescribes to implement the following cipher suites for the communication between EV and Charging Station: TLS_ECDH_ECDSA_WITH_AES_128_**CBC**_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_**CBC**_SHA256
A00.FR.423		The Charging Station and CSMS 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 [10].

ID	Precondition	Requirement definition
A00.FR.425	A00.FR.424 AND If the CSMS detects that the Charging Station only allows connections using one of these suites	The CSMS SHALL terminate the connection.
A00.FR.426	A00.FR.424 AND The Charging Station detects that the CSMS only allows connections using one of these suites	The Charging Station SHALL trigger an InvalidTLSCipherSuite security event AND terminate the connection (See part 2 appendices for the full list of security events).
A00.FR.427		A unique Charging Station certificate SHALL be used for each Charging Station.
A00.FR.428		The Charging Station Certificate MAY be the same certificate as the SECC Certificate in ISO15118-2, used to set up a TLS connection between the Charging Station and an Electric Vehicle.

1.4. Keys used in OCPP

This section is normative.

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

Table 19. Certificates used in the OCPP security specification

Certificate	Private Key Stored At	Description
CSMS Certificate	CSMS	Key used to authenticate the CSMS.
Charging Station Certificate	Charging Station	Key used to authenticate the Charging Station.
Firmware Signing Certificate	Manufacturer	Key used to verify the firmware signature.
SECC Certificate	Charging Station	Certificate used by ISO15118-2 to set up a TLS connection between the Charging Station and an Electric Vehicle.

1.4.1. Certificate Properties

This section is normative.

Table 20. 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 [17]. 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 [12], 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.

ID	Precondition	Requirement definition
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 CSMS certificate, the subject field SHALL contain the FQDN of the endpoint of the server in the CN (`commonName`) RDN.
A00.FR.511		For the Charging Station certificate, the subject field SHALL contain a CN (`commonName`) RDN which consists of the unique serial number of the Charging Station. This serial number SHALL NOT be in the format of a URL or an IP address so that Charging Station certificates can be differentiated from CSMS certificates. Note: According to RFC 2818, if a `subjectAltName` extension of type `dnsName` is present, that must be used as the identity. This would be incompliant with OCPP and ISO 15118. Therefore it SHOULD NOT be used in Charging Station and CSMS certificates. It is allowed to use the subjectAltName extension of type dnsName for a CSMS, when the CSMS has multiple network paths to reach 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 [19] SHOULD be used to restrict the usage of the certificate to the operations for which it will be used.
A00.FR.513		If the Charging Station Certificate is also used as SECC Certificate in the ISO 15118 protocol, the certificate SHOULD also meet the requirements in ISO15118-2.
A00.FR.514		For all certificates it is strongly RECOMMENDED NOT to use the X.509 Extended Key Usage extension, to be compatible with the ISO 15118 standard. There are alternative mechanisms available.

1.4.2. Certificate Hierarchy

This section is normative.

The OCPP protocol supports the use of two separate certificate hierarchies:

1. The Charging Station Operator hierarchy which contains the CSMS, and Charging Station certificates.
2. The Manufacturer hierarchy which contains the Firmware Signing certificate.

The CSMS can update the CSO root certificates stored on the Charging Station using the InstallCertificateRequest message.

Table 21. Certificate Hierarchy requirements

ID	Precondition	Requirement definition
A00.FR.601		The Charging Station Operator MAY act as a certificate authority for the Charging Station Operator hierarchy
A00.FR.602	A00.FR.601	The Charging Station Operator MAY for instance follow the certificate hierarchy described in Appendices E and F of ISO15118-2 and use the CSO Sub-CA 2 certificate to sign the CSMS and Charging Station certificates. This could give the advantage that the online verification of Charging Station client side certificates can be done within the Charging Station Operator's networks, simplifying the network architecture.
A00.FR.603		The private keys belonging to the CSO root certificates MUST be well protected.
A00.FR.604		As the Manufacturer is usually a separate organization from the Charging Station Operator, a trusted third party SHOULD be used as a certificate authority. This is essential to have non-repudiation of firmware images.

1.5. Certificate Revocation

This section is normative.

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 22. Recommended revocation methods for the different certificates.

Certificate	Revocation
CSMS certificate	Fast expiration
Charging Station certificate	Online verification
Firmware Signing certificate	Online verification

Table 23. Certificate Revocation requirements

ID	Precondition	Requirement definition
A00.FR.701		Fast expiration SHOULD be used to revoke the CSMS certificate. (See Note 1)
A00.FR.702		The CSMS SHOULD use online certificate verification to verify the validity of the Charging Station certificates.
A00.FR.703		It is RECOMMENDED that a separate certificate authority server is used to manage the certificates.
A00.FR.704	A00.FR.703	This server SHOULD also keep track of which certificates have been revoked.
A00.FR.705		The CSMS SHALL verify the validity of the certificate with the certificate authority server. (See Note 2)
A00.FR.707		Prior to providing the certificate for firmware validation to the Charging Station, the CSMS 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 CSO itself (see section Certificate Hierarchy). This prevents the Charging Stations from needing to implement revocation lists or online certificate verification. This simplifies the implementation of certificate management at the Charging Station and reduces communication costs at the Charging Station 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 Charging Station to connect to a "fake" CSMS. By using fast expiration, the time a Charging Station is vulnerable is greatly reduced.

The Charging Station always communicates with the Certificate Authority through the CSMS, this way, if the Charging Station is compromised, the Charging Station cannot attack the CA directly.

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

1.6. Installation

This section is normative.

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

Table 24. Certificate Installation requirements

ID	Precondition	Requirement definition
A00.FR.801		It is RECOMMENDED that the manufacturer initializes the Charging Station 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	They SHOULD be sent to the CSO over a secure channel, so that the CSO can import them in the CSMS
A00.FR.804	If Charging Station certificates are used.	The manufacturer MAY sign these using their own certificate.
A00.FR.805	A00.FR.804	It is RECOMMENDED that the CSO immediately updates the credentials after installation using the methods described in Section A01 - Update Charging Station Password for HTTP Basic Authentication or A02 - Update Charging Station Certificate by request of CSMS.
A00.FR.806	Before the 'factory credentials' have been updated	The CSMS MAY restrict the functionality that the Charging Station can use. The CSMS can use the BootNotification state: Pending for this. During the Pending state, the CSMS can update the credentials.

2. Use cases & Requirements

A01 - Update Charging Station Password for HTTP Basic Authentication

Table 25. A01 - Password Management

No.	Type	Description
1	**Name**	Update Charging Station Password for HTTP Basic Authentication
2	**ID**	A01
	Functional block	A. Security
3	**Objective(s)**	This use case defines how to use the BasicAuthPassword, the password used to authenticate Charging Stations in the Basic and TLS with Basic Authentication security profiles.
4	**Description**	To enable the CSMS to configure a new password for HTTP Basic Authentication, the CSMS can send a new value for the `BasicAuthPassword` Configuration Variable.
	Actors	Charging Station, CSMS
	Scenario description	**1.** The CSMS sends a SetVariablesRequest(ComponentName=SecurityCtrlr, VariableName=BasicAuthPassword) to the Charging Station. **2.** The Charging Station responds with SetVariablesResponse and the status *Accepted*. **3.** The Charging Station disconnects its current connection. (Storing any queued messages) **4.** The Charging Station connects to the CSMS 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 Charging Station has reconnected to the CSMS with the new password. **Failure postcondition:** If the Charging Station responds to the SetVariablesRequest with a SetVariablesResponse with a status other than *Accepted*, the Charging Station will keep using the old credentials. The CSMS might treat the Charging Station differently, e.g. by not accepting the Charging Station's boot notifications.

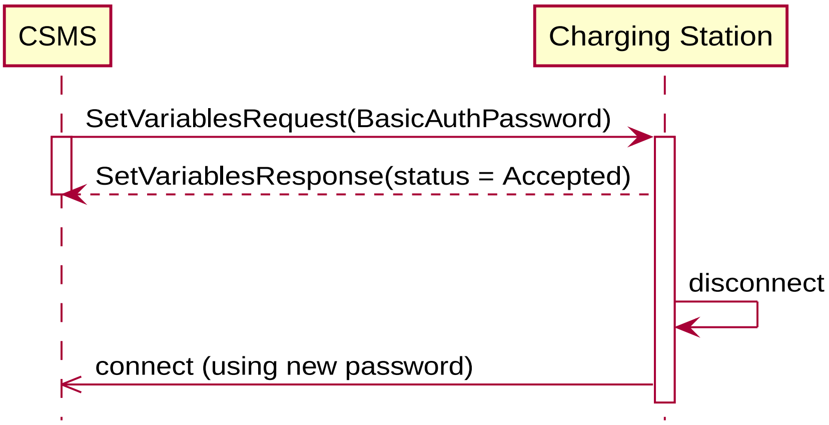
CSMS
Charging Station
SetVariablesRequest(BasicAuthPassword)
SetVariablesResponse(status = Accepted)
disconnect
connect (using new password)

Figure 5. Update Charging Station Password for HTTP Basic Authentication (happy flow)

No.	Type	Description
7	**Error handling**	n/a
8	**Remark(s)**	n/a

A01 - Update Charging Station Password for HTTP Basic Authentication - Requirements

Table 26. A01 - Update Charging Station Password for HTTP Basic Authentication - Requirements

ID	Precondition	Requirement definition
A01.FR.01		The password SHALL be stored in the configuration variable `BasicAuthPassword`.

ID	Precondition	Requirement definition
A01.FR.02		To set a Charging Station's basic authorization password via OCPP, the CSMS SHALL send the Charging Station a SetVariablesRequest message with the `BasicAuthPassword` Configuration Variable.
A01.FR.03	A01.FR.02 AND The Charging Station responds to this SetVariablesRequest with a SetVariablesResponse with status *Accepted*.	The CSMS SHALL assume that the authorization key change was successful, and no longer accept the credentials previously used by the Charging Station.
A01.FR.04	A01.FR.02 AND The Charging Station responds to this SetVariablesRequest with a SetVariablesResponse with status other than *Accepted*	The CSMS SHALL assume that the Charging Station has NOT changed the password. Therefore the CSMS SHALL keep accepting the old credentials.
A01.FR.05	A01.FR.04	While the CSMS SHALL still accepts a connection from the Charging Station, it MAY restrict the functionality that the Charging Station can use. The CSMS can use the BootNotification state: Pending for this. During the Pending state, the CSMS can for example retry to update the credentials.
A01.FR.06		Different passwords SHOULD be used for different Charging Stations.
A01.FR.07		Passwords SHOULD be generated randomly to ensure that the passwords have sufficient entropy.
A01.FR.08		the CSMS SHOULD only store salted password hashes, not the passwords themselves.
A01.FR.09		the CSMS SHOULD NOT put the passwords in clear-text in log files or debug information. In this way, if the CSMS is compromised not all Charging Station password will be immediately compromised.
A01.FR.10		On the Charging Station 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 Charging Station SHALL log the change of an `BasicAuthPassword` in the Security log.
A01.FR.12	A01.FR.11	The Charging Station SHALL NOT disclose the content of the BasicAuthPassword in its logging. This is to prevent exposure of key material to persons that may have access to a diagnostics file.

A02 - Update Charging Station Certificate by request of CSMS

Table 27. A02 - Update Charging Station Certificate by request of CSMS

No.	Type	Description
1	**Name**	Update Charging Station Certificate by request of CSMS
2	**ID**	A02
	Functional block	A. Security
3	**Objective(s)**	To facilitate the management of the Charging Station client side certificate, a certificate update procedure is provided.
4	**Description**	The CSMS requests the Charging Station to update its key using TriggerMessageRequest with the *requestedMessage* field set to SignChargingStationCertificate (or SignV2GCertificate for separate 15118 certificate).
	Actors	Charging Station, CSMS, Certificate Authority Server

No.	Type	Description
	Scenario description	**1.** The CSMS requests the Charging Station to update its certificate using the TriggerMessageRequest with the *requestedMessage* field set to SignChargingStationCertificate (or SignV2GCertificate for separate 15118 certificate). **2.** The Charging Station responds with TriggerMessageResponse **3.** The Charging Station generates a new public / private key pair. **4.** The Charging Station sends a SignCertificateRequest to the CSMS containing the applicable CertificateSigningUse . **5.** The CSMS responds with SignCertificateResponse, with status *Accepted*. **6.** The CSMS 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 CSMS. **9.** The CSMS sends CertificateSignedRequest to the Charging Station. **10.** The Charging Station verifies the Signed Certificate. **11.** The Charging Station responds with CertificateSignedResponse to the CSMS with the status *Accepted* or *Rejected*.
5	**Prerequisite(s)**	The standard configuration variable `OrganizationName` MUST be set.
6	**Postcondition(s)**	**Successful postcondition:** New Client Side certificate installed in the Charging Station. **Failure postcondition:** New Client Side certificate is rejected and discarded.

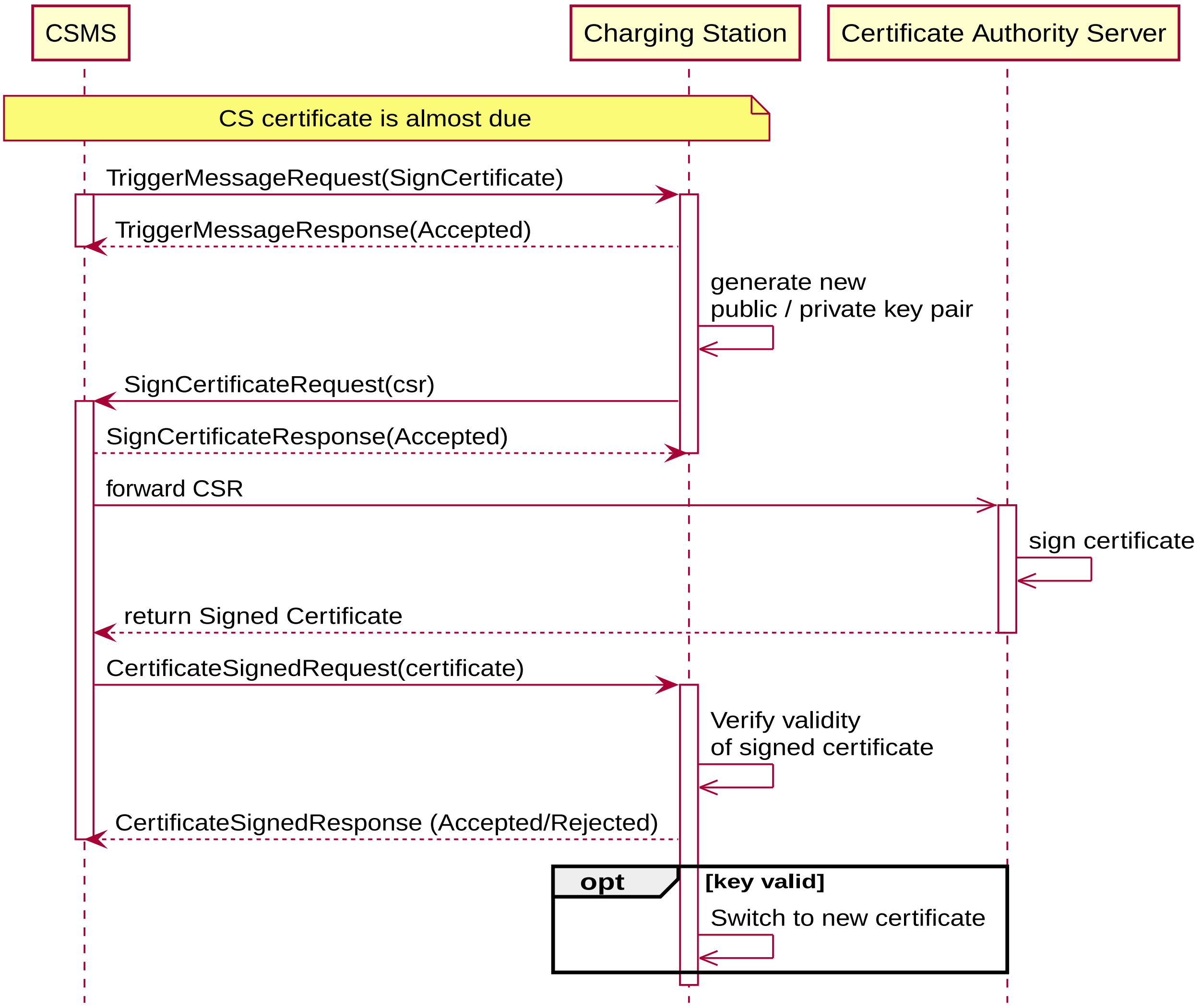
CSMS
Charging Station
Certificate Authority Server
CS certificate is almost due
TriggerMessageRequest(SignCertificate)
TriggerMessageResponse(Accepted)
generate new
public / private key pair
SignCertificateRequest(csr)
SignCertificateResponse(Accepted)
forward CSR
sign certificate
return Signed Certificate
CertificateSignedRequest(certificate)
Verify validity
of signed certificate
CertificateSignedResponse (Accepted/Rejected)
opt
[key valid]
Switch to new certificate

Figure 6. Update Charging Station Certificate

7	**Error handling**	The CSMS accepts the CSR request from the Charging Station, before forwarding it to the CA. But when the CA cannot be reached, or rejects the CSR, the Charging Station will never known. The CSMS 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 Charging Station is not correct, according to the CA. In both cases this is something an operator at the CSO 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 Charging Station 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 Charging Station Operator may act as a certificate authority for the Charging Station Operator hierarchy. 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 CSO, the CSO sends it back to the Charging Station in the CertificateSignedRequest message. The certificate authority SHOULD implement strong measures to keep the certificate signing private keys secure. Even though the messages CertificateSignedRequest (see use cases A02 and A03) and InstallCertificateRequest (use case M05 - Install CA Certificate in a Charging Station) are both used to send certificates, their purposes are different. CertificateSignedRequest is used to return the the Charging Stations own public certificate and V2G certificate(s) signed by a Certificate Authority. InstallCertificateRequest is used to install Root certificates. For V2G certificate handling see use cases M03 - Retrieve list of available certificates from a Charging Station, M04 - Delete a specific certificate from a Charging Station and M06 - Get Charging Station Certificate status.

A02 - Update Charging Station Certificate by request of CSMS - Requirements

Table 28. A02 - Requirements

ID	Precondition	Requirement definition
A02.FR.01		A key update SHOULD be performed after installation of the Charging Station, to change the key from the one initially provisioned by the manufacturer (possibly a default key).
A02.FR.02	After sending a TriggerMessageResponse.	The Charging Station SHALL generate a new public / private key pair using one of the key generation functions described in Section 4.2.1.3 of [16].
A02.FR.03	A02.FR.02	The Charging Station SHALL send the public key in form of a Certificate Signing Request (CSR) as described in RFC 2986 [22] and then PEM encoded, using the SignCertificateRequest message.
A02.FR.04		The CSMS SHOULD NOT sign the certificate itself, but instead forwards the CSR to a dedicated certificate authority server managing the certificates for the Charging Station infrastructure. The dedicated authority server MAY be operated by the CSO.
A02.FR.05		The private key generated by the Charging Station during the key update process SHALL NOT leave the Charging Station at any time, and SHALL NOT be readable via OCPP or any other (remote) communication connection.
A02.FR.06		The Charging Station SHALL verify the validity of the signed certificate in the CertificateSignedRequest message, checking at least the period when the certificate is valid, the properties in Certificate Properties, and that it is part of the Charging Station Operator certificate hierarchy as described in Certificate Hierarchy.
A02.FR.07	If the certificate is not valid.	The Charging Station SHALL discard the certificate, and trigger an InvalidChargingStationCertificate security event (See part 2 appendices for the full list of security events).
A02.FR.08		The Charging Station SHALL switch to the new certificate as soon as the current date and time is after the 'Not valid before' field in the certificate.

ID	Precondition	Requirement definition
A02.FR.09	If the Charging Station contains more than one valid certificate of the *ChargingStationCertificate* type.	The Charging Station SHALL use the newest certificate, as measured by the start of the validity period.
A02.FR.10	A02.FR.09 AND When the Charging Station has validated that the new certificate works	The Charging Station MAY discard the old certificate. It is RECOMMENDED to store old certificates for one month, as fallback.
A02.FR.11	Upon receipt of a SignCertificateRequest AND It is able to process the request	The CSMS SHALL set status to *Accepted* in the SignCertificateResponse.
A02.FR.12	Upon receipt of a SignCertificateRequest AND It is NOT able to process the request	The CSMS SHALL set status to *Rejected* in the SignCertificateResponse.
A02.FR.13	When using different certificates for 15118 connections and the Charging Station to CSMS connection	The Charging Station SHALL set the certificateType field in the SignCertificateRequest to the certificate for which the update was triggered.
A02.FR.14	When receiving a SignCertificateRequest with certificateType included	It is RECOMMENDED for the CSMS to set the certificateType field in the CertificateSignedRequest to the type of certificate in the SignCertificateRequest.
A02.FR.15	If the Charging Station contains more than one valid V2G certificate, derived from the same root certificate.	The Charging Station SHALL use the newest certificate, as measured by the start of the validity period.
A02.FR.16	If the configuration variable MaxCertificateChainSize is implemented AND The Charging Station receives a CertificateSignedRequest message with a certificate (chain) with with a size that exceeds the set value configured at MaxCertificateChainSize	The Charging Station SHALL respond with a CertificateSignedResponse message with status *Rejected* .

A03 - Update Charging Station Certificate initiated by the Charging Station

Table 29. A03 - Update Charging Station Certificate initiated by the Charging Station

No.	Type	Description
1	**Name**	Update Charging Station Certificate initiated by the Charging Station
2	**ID**	A03
	Functional block	A. Security
3	**Objective(s)**	To facilitate the management of the Charging Station client side certificate, a certificate update procedure is provided.
4	**Description**	The Charging Station detects that the certificate (ChargingStationCertificate or V2GCertificate for 15118) it is using will expire in one month. The Charging Station initiates the process to update its key using SignCertificateRequest, indicating the requested certificate in the CertificateSigningUse field.
	Actors	Charging Station, CSMS, Certificate Authority Server

No.	Type	Description
	Scenario description	**1.** The Charging Station detects that the Charging Station certificate is due to expire. **2.** The Charging Station generates a new public / private key pair. **3.** The Charging Station sends a SignCertificateRequest to the CSMS containing the applicable CertificateSigningUse. **4.** The CSMS responds with a SignCertificateResponse, with status *Accepted*. **5.** The CSMS 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 CSMS. **8.** The CSMS sends a CertificateSignedRequest to the Charging Station. **9.** The Charging Station verifies the Signed Certificate. **10.** The Charging Station responds with a CertificateSignedResponse to the CSMS with the status *Accepted* or *Rejected*.
5	**Prerequisite(s)**	The standard configuration variable `OrganizationName` MUST be set.
6	**Postcondition(s)**	**Successful postcondition:** New Client Side certificate installed in the Charging Station. **Failure postcondition:** New Client Side certificate is rejected and discarded.

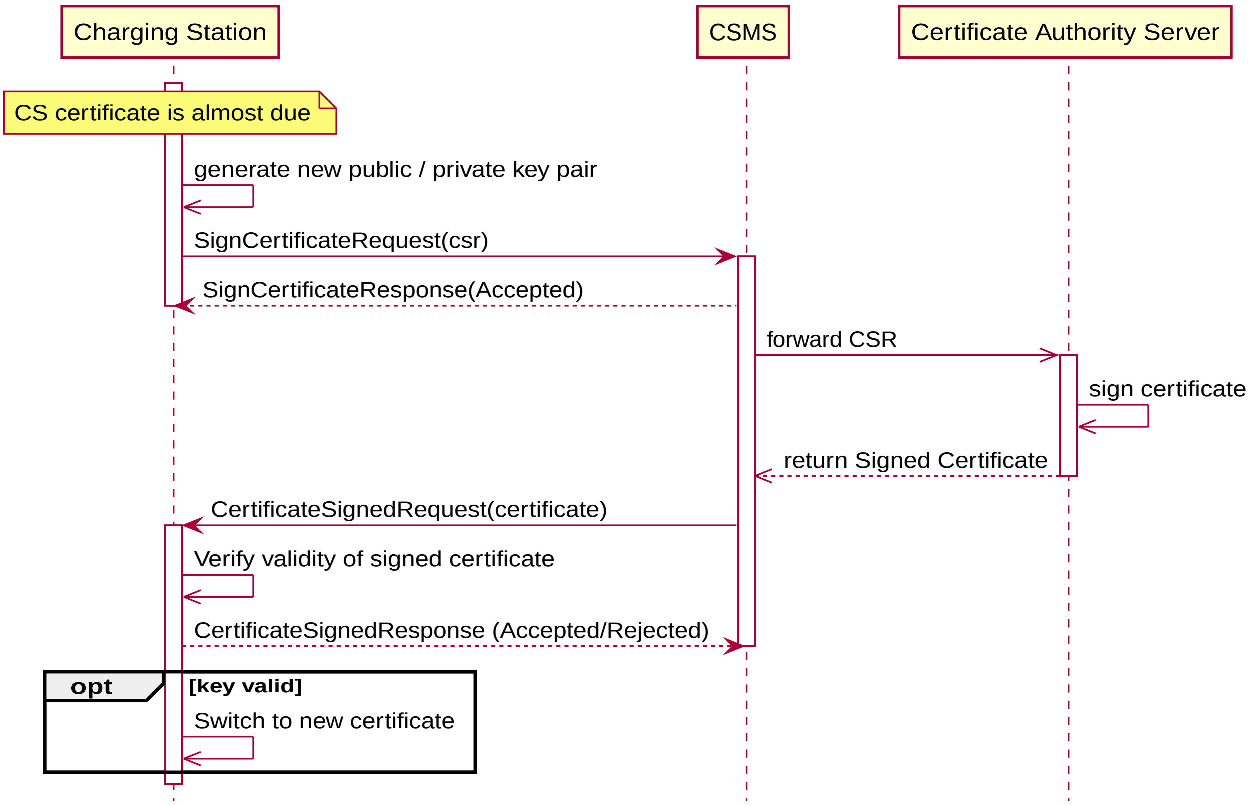
Charging Station
CSMS
Certificate Authority Server
CS certificate is almost due
generate new public / private key pair
SignCertificateRequest(csr)
SignCertificateResponse(Accepted)
forward CSR
sign certificate
return Signed Certificate
CertificateSignedRequest(certificate)
Verify validity of signed certificate
CertificateSignedResponse (Accepted/Rejected)
opt
[key valid]
Switch to new certificate

Figure 7. Update Charging Station Certificate initiated by Charging Station

7	**Error handling**	The CSMS accepts the CSR request from the Charging Station, before forwarding it to the CA. But when the CA cannot be reached, or rejects the CSR, the Charging Station will never known. The CSMS 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 Charging Station is not correct, according to the CA. In both cases this is something an operator at the CSO 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 Charging Station 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 Charging Station Certificate by request of CSMS apply.

A03 - Update Charging Station Certificate initiated by the Charging Station - Requirements

Table 30. A03 - Requirements

ID	Precondition	Requirement definition
A03.FR.01		A key update MAY be performed after installation of the Charging Station, to change the key from the one initially provisioned by the manufacturer (possibly a default key).
A03.FR.02	When the Charging Station detects that the current Charging Station certificate will expire in one month.	The Charging Station SHALL generate a new public / private key pair using one of the key generation functions described in Section 4.2.1.3 of [16].
A03.FR.03	A03.FR.02	The Charging Station SHALL send the public key in form of a Certificate Signing Request (CSR) as described in RFC 2986 [22] and then PEM encoded, using the SignCertificateRequest message.
A03.FR.04		The CSMS SHOULD NOT sign the certificate itself, but instead forwards the CSR to a dedicated certificate authority server managing the certificates for the Charging Station infrastructure. The dedicated authority server MAY be operated by the CSO.
A03.FR.05		The private key generated by the Charging Station during the key update process SHALL NOT leave the Charging Station at any time, and SHALL NOT be readable via OCPP or any other (remote) communication connection.
A03.FR.06		The Charging Station SHALL verify the validity of the signed certificate in the CertificateSignedRequest message, checking at least the period when the certificate is valid, the properties in Certificate Properties, and that it is part of the Charging Station Operator certificate hierarchy as described in Certificate Hierarchy.
A03.FR.07	If the certificate is not valid.	The Charging Station SHALL discard the certificate, and trigger an InvalidChargingStationCertificate security event (See part 2 appendices for the full list of security events).
A03.FR.08		The Charging Station 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 Charging Station contains more than one valid certificate of the *ChargingStationCertificate* type.	The Charging Station SHALL use the newest certificate, as measured by the start of the validity period.
A03.FR.10	A03.FR09 AND When the Charging Station has validated that the new certificate works	The Charging Station MAY discard the old certificate. It is RECOMMENDED to store old certificates for one month, as fallback.
A03.FR.11	Upon receipt of a SignCertificateRequest AND It is able to process the request	The CSMS SHALL set status to *Accepted* in the SignCertificateResponse.
A03.FR.12	Upon receipt of a SignCertificateRequest AND It is NOT able to process the request	The CSMS SHALL set status to *Rejected* in the SignCertificateResponse.
A03.FR.13	When using different certificates for 15118 connections and the Charging Station to CSMS connection	The Charging Station SHALL include the certificateType field in the SignCertificateRequest to specify which certificate it wants to update.
A03.FR.14	When receiving a SignCertificateRequest with certificateType included	It is RECOMMENDED for the CSMS to set the certificateType field in the CertificateSignedRequest to the type of certificate in the SignCertificateRequest.
A03.FR.15	If the Charging Station contains more than one valid V2G certificate, derived from the same root certificate.	The Charging Station SHALL use the newest certificate, as measured by the start of the validity period.

ID	Precondition	Requirement definition
A03.FR.16	If the configuration variable MaxCertificateChainSize is implemented AND The Charging Station receives a CertificateSignedRequest message with a certificate (chain) with with a size that exceeds the set value configured at MaxCertificateChainSize	The Charging Station SHALL respond with a CertificateSignedResponse message with status *Rejected* .

A04 - Security Event Notification

Table 31. A04 - Security Event Notification

No.	Type	Description
1	**Name**	Security Event Notification
2	**ID**	A04
	Functional block	A. Security
3	**Objective(s)**	To inform the CSMS of critical security events.
4	**Description**	This use case allows the Charging Station to immediately inform the CSMS of changes in the system security.
	Actors	CSMS, Charging Station
	Scenario description	**1.** A *critical* security event happens. **2.** The Charging Station sends a SecurityEventNotificationRequest to the CSMS. **3.** The CSMS responds with SecurityEventNotificationResponse to the Charging Station.
5	**Prerequisite(s)**	n/a
6	**Postcondition(s)**	The Charging Station *successfully* informs the CSMS of critical security events by sending a SecurityEventNotificationRequest to the CSMS.

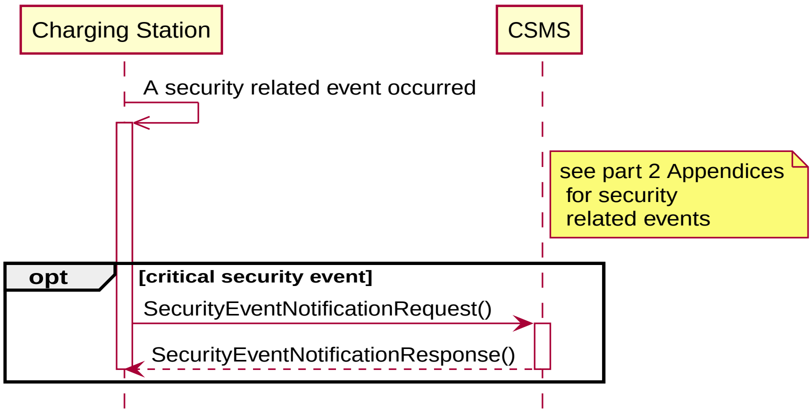
Charging Station
CSMS
A security related event occurred
see part 2 Appendices for security related events
opt
[critical security event]
SecurityEventNotificationRequest()
SecurityEventNotificationResponse()

Figure 8. Security Event Notification

7	**Error handling**	n/a
8	**Remark(s)**	A list of security related events and their 'criticality' is provided in the Appendices (*Appendix 1. Security Events*)

A04 - Security Event Notification - Requirements

Table 32. A04 - Security Event Notification - Requirements

ID	Precondition	Requirement definition	Note
A04.FR.01	When a *critical* security event happens	The Charging Station SHALL inform the CSMS of the security events by sending a SecurityEventNotificationRequest to the CSMS.	
A04.FR.02	A04.FR.01 AND the Charging Station is disconnected.	Security event notifications MUST be queued with a guaranteed delivery at the CSMS.	
A04.FR.03	A04.FR.01	The CSMS SHALL confirm the receipt of the notification using the SecurityEventNotificationResponse message.	
A04.FR.04	When a security event happens (also non-critical)	The Charging Station SHALL store the security event in a security log.	It is recommended to implement this log in a rolling format.

A05 - Upgrade Charging Station Security Profile

Table 33. A05 - Upgrade Charging Station Security Profile

No.	Type	Description
1	**Name**	Upgrade Charging Station Security Profile
2	**ID**	A05
	Functional block	A. Security
3	**Objective(s)**	The CSO wants to increase the security of the OCPP connection between CSMS and a Charging Station.
4	**Description**	Use case when migrating from OCPP 1.6 without security profiles to OCPP 1.6 with security profiles or OCPP 2.0.1 Before migrating to a security profile the prerequisites, like installed certificates or password need to be configured.
	Actors	CSMS, Charging Station
	Scenario description	**1.** The CSMS sets a new value for the `NetworkConfigurationPriority` Configuration Variable via SetVariablesRequest, such that the NetworkConnectionProfile for the new (higher) security profile becomes first in the list and the existing connection profile becomes second in the list. **2.** The Charging Station responds with a SetVariablesResponse with status *Accepted* **3.** The CSMS sends a ResetRequest(OnIdle) **4.** The Charging Station reboots and connects via the new primary NetworkConnectionProfile
5	**Prerequisite(s)**	The CSO ensures that a NetworkConnectionProfile has been set using (higher) security profile AND that the prerequisite(s) for going to a higher security profile are met before sending the command to change to a higher security profile.
6	**Postcondition(s)**	The Charging Station was successfully upgraded to a higher security profile.

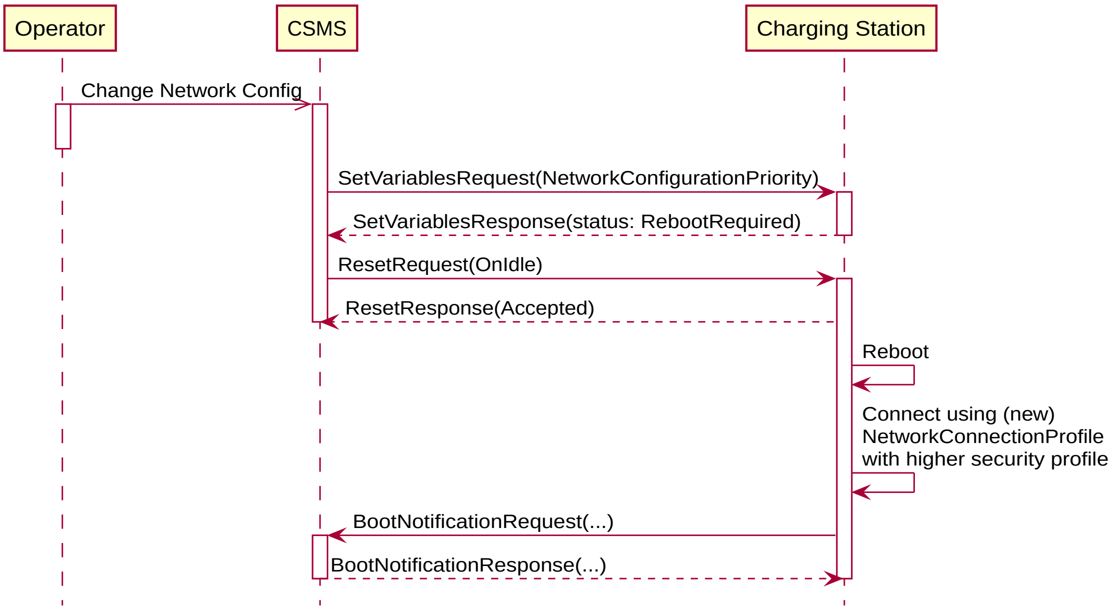
Operator
CSMS
Charging Station
Change Network Config
SetVariablesRequest(NetworkConfigurationPriority)
SetVariablesResponse(status: RebootRequired)
ResetRequest(OnIdle)
ResetResponse(Accepted)
Reboot
Connect using (new)
NetworkConnectionProfile
with higher security profile
BootNotificationRequest(...)
BootNotificationResponse(...)

Figure 9. Upgrade Charging Station Security Profile

7	**Error handling**	n/a
8	**Remark(s)**	For security reasons it is not allowed to revert to a lower Security Profile using OCPP.

A05 - Upgrade Charging Station Security Profile - Requirements

Table 34. A05 - Upgrade Charging Station Security Profile

ID	Precondition	Requirement definition
A05.FR.02	The Charging Station receives SetVariablesRequest for `NetworkConfigurationPriority` containing a profile slot for a NetworkConnectionProfile with a 'securityProfile' value higher than the current value AND new value is 2 or 3 AND No valid CSMSRootCertificate installed	The Charging Station SHALL respond with SetVariablesResponse(Rejected), and not update the value for `SecurityProfile` and/or reconnect to the CSMS.
A05.FR.03	The Charging Station receives SetVariablesRequest for `NetworkConfigurationPriority` containing a profile slot for a NetworkConnectionProfile with a 'securityProfile' value higher than the current value AND new value is 3 AND No valid ChargingStationCertificate installed	The Charging Station SHALL respond with SetVariablesResponse(Rejected), and not update the value for `SecurityProfile` and/or reconnect to the CSMS.
A05.FR.04	The Charging Station receives SetVariablesRequest for `NetworkConfigurationPriority` containing profile slots for NetworkConnectionProfiles with a 'securityProfile' value equal to or higher than the current value AND all prerequisites are met	The Charging Station SHALL respond with SetVariablesResponse(Accepted)
A05.FR.05	A05.FR.04 AND After a reboot	The Charging Station SHALL begin connecting to the first entry of `NetworkConfigurationPriority`
A05.FR.06	A05.FR.05 AND The Charging Station successfully connected to the CSMS using the (new) NetworkConnectionProfile	The Charging Station SHALL update the value of the configuration variable `SecurityProfile` AND it SHALL remove all NetworkConnectionProfiles with a lower securityProfile than stored at `SecurityProfile` AND update `NetworkConfigurationPriority` accordingly.
A05.FR.07	A05.FR.06	The CSMS SHALL NOT allow the Charging Station to connect with a lower security profile anymore.