L. FirmwareManagement

1. Introduction

This Functional Block describes the functionality that enables a CSO to update the firmware of a Charging Station.

When a Charging Station needs to be updated with new firmware, the CSMS informs the Charging Station of the time at which the Charging Station can start downloading the new firmware. The Charging Station SHALL notify the CSMS after each step as it downloads and installs the new firmware.

2. Use cases & Requirements

L01 - Secure Firmware Update

Table 192. L01 - Secure Firmware Update

No.	Type	Description
1	**Name**	Secure Firmware Update
2	**ID**	L01
	Functional block	L. Firmware Management
3	**Objective(s)**	Download and install a Secure firmware update.
4	**Description**	Illustrate how a Charging Station processes a Secure firmware update.
	Actors	CSMS, Charging Station, Charging Station Manufacturer
	Scenario description	**1.** The CSMS sends an UpdateFirmwareRequest message that contains the location of the firmware, the time after which it should be retrieved, and information on how many times the Charging Station should retry downloading the firmware. **2.** The Charging Station verifies the validity of the certificate against the Manufacturer root certificate. **3.** If the certificate is valid, the Charging Station starts downloading the firmware, and sends a FirmwareStatusNotificationRequest with status Downloading. If the certificate is not valid or could not be verified, the Charging Station aborts the firmware update process and sends a UpdateFirmwareResponse with status InvalidCertificate and a SecurityEventNotificationRequest with the security event InvalidFirmwareSigningCertificate (See part 2 appendices for the full list of security events). **4.** If the Firmware successfully downloaded, the Charging Station sends a FirmwareStatusNotificationRequest with status Downloaded. Otherwise, it sends a FirmwareStatusNotificationRequest with status DownloadFailed. **5.** If the verification is successful, the Charging Station sends a FirmwareStatusNotificationRequest with status Installing. If the verification of the firmware fails or if a signature is missing entirely, the Charging Station sends a FirmwareStatusNotificationRequest with status InvalidSignature and a SecurityEventNotificationRequest with the security event InvalidFirmwareSignature (See part 2 appendices for the full list of security events). **6.** If the installation is successful, the Charging Station sends a FirmwareStatusNotificationRequest with status Installed. Otherwise, it sends a FirmwareStatusNotificationRequest with status InstallationFailed.
	Alternative scenario(s)	L02 - Non-Secure Firmware Update
5	**Prerequisite(s)**	The Charging Station Manufacturer provided a firmware update.
6	**Postcondition(s)**	**Successful postcondition:** The firmware is updated and the Charging Station is in *Installed* status. **Failure postconditions:** The certificate is not valid or could not be verified and the Charging Station is in *InvalidCertificate* status. Downloading the firmware failed and the Charging Station is in *DownloadFailed* status. The verification of the firmware's digital signature failed and the Charging Station is in *InvalidSignature* status. The installation of the firmware is not successful and the Charging Station is in *InstallationFailed* status.

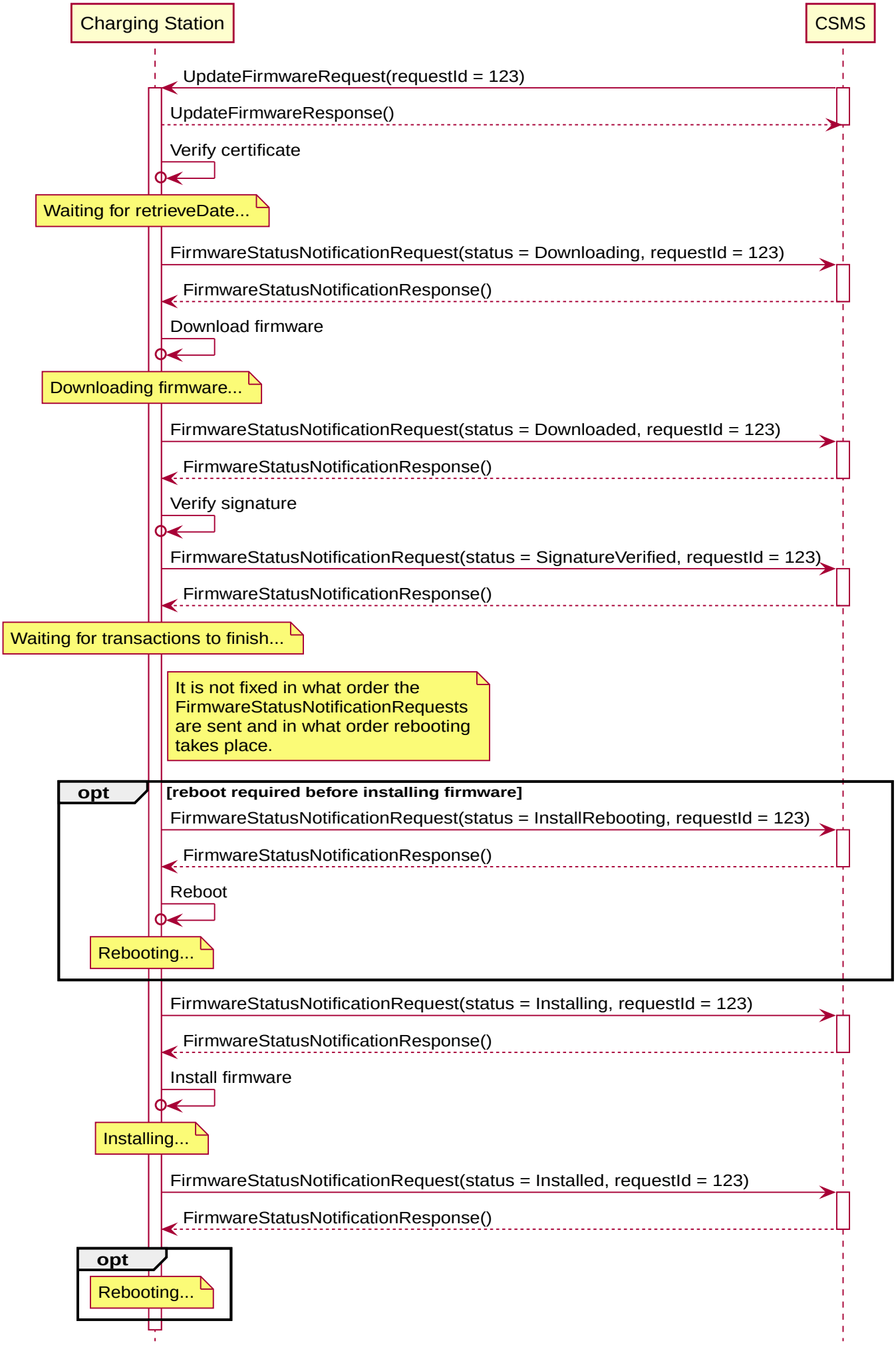
Charging Station
CSMS
UpdateFirmwareRequest(requestId = 123)
UpdateFirmwareResponse()
Verify certificate
Waiting for retrieveDate...
FirmwareStatusNotificationRequest(status = Downloading, requestId = 123)
FirmwareStatusNotificationResponse()
Download firmware
Downloading firmware...
FirmwareStatusNotificationRequest(status = Downloaded, requestId = 123)
FirmwareStatusNotificationResponse()
Verify signature
FirmwareStatusNotificationRequest(status = SignatureVerified, requestId = 123)
FirmwareStatusNotificationResponse()
Waiting for transactions to finish...
It is not fixed in what order the FirmwareStatusNotificationRequests are sent and in what order rebooting takes place.
opt
[reboot required before installing firmware]
FirmwareStatusNotificationRequest(status = InstallRebooting, requestId = 123)
FirmwareStatusNotificationResponse()
Reboot
Rebooting...
FirmwareStatusNotificationRequest(status = Installing, requestId = 123)
FirmwareStatusNotificationResponse()
Install firmware
Installing...
FirmwareStatusNotificationRequest(status = Installed, requestId = 123)
FirmwareStatusNotificationResponse()
opt
Rebooting...

Figure 116. Sequence diagram secure firmware upgrade (happy flow)

7	**Error handling**	n/a
8	**Remark(s)**	As an example in this use case the requestId = 123, but this could be any value. Measures SHOULD be taken to secure the firmware when it is stored on a server or workstation. The Charging Station has a required Configuration Variable that reports which file transfer protocols it supports: `FileTransferProtocols` When migrating to a new version of OCPP it is RECOMMENDED to install a fallback NetworkConnectionProfile with the new configuration. The requirements for the Firmware Signing Certificate are described in the: Certificate Properties section. The manufacturer SHALL NOT use intermediate certificates for the firmware signing certificate in the Charging Station. FTP needs to be able to use Passive FTP, to be able to transverse over as much different typologies as possible.

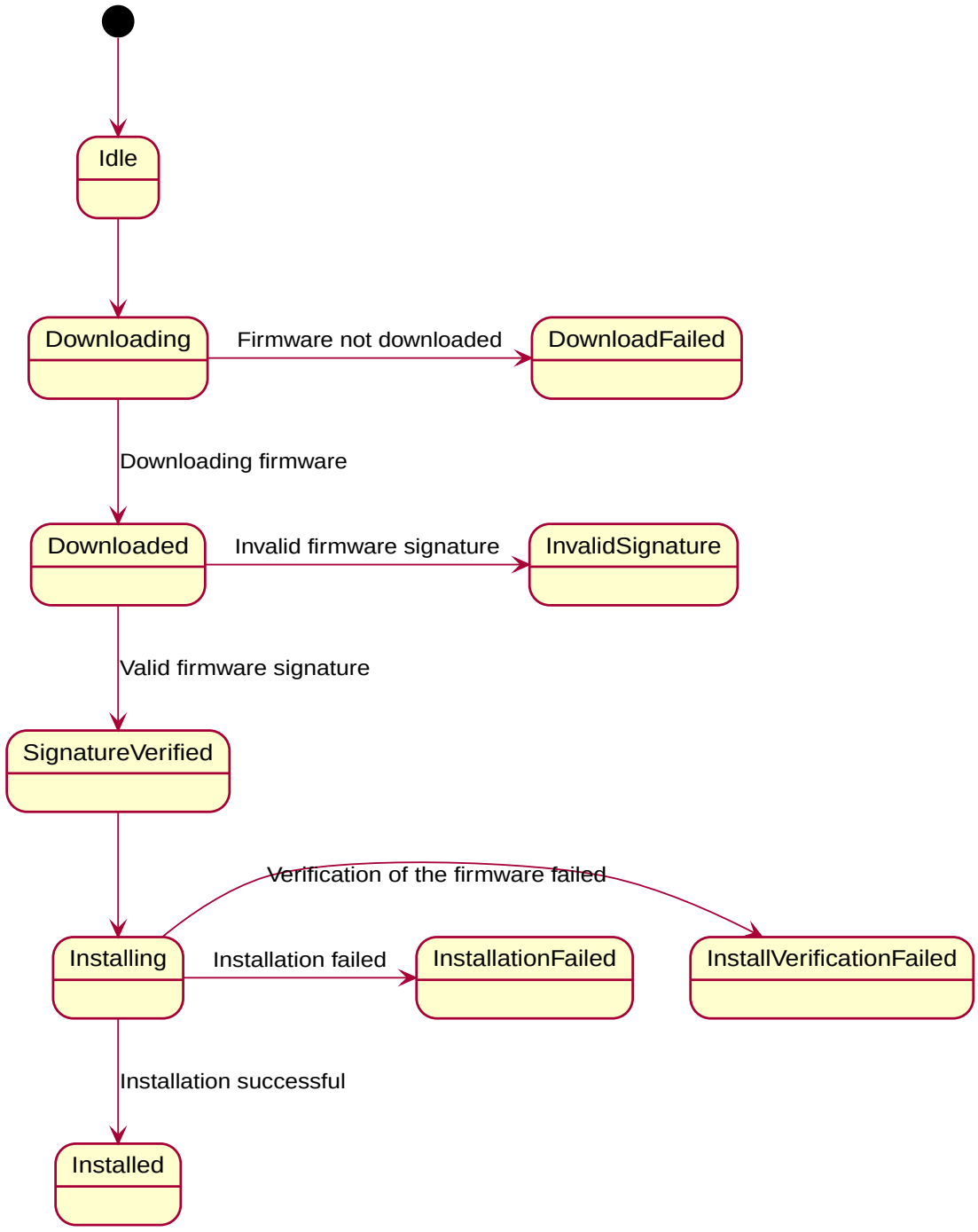

Figure 117. Firmware update process

L01 - Secure Firmware Update - Requirements

Table 193. L01 - Requirements

ID	Precondition	Requirement definition	Note
L01.FR.01	Whenever the Charging Station enters a new state in the firmware update process.	The Charging Station SHALL send a FirmwareStatusNotificationRequest message to the CSMS with this new status. What reason to use is described in the description of FirmwareStatusEnumType.	
L01.FR.02	When the Charging Station enters the Invalid Certificate state in the firmware process.	The Charging Station SHALL send a SecurityEventNotificationRequest message to the CSMS with the security event InvalidFirmwareSigningCertificate (See part 2 appendices for the full list of security events).	

ID	Precondition	Requirement definition	Note
L01.FR.03	When the Charging Station enters the Invalid Signature state.	The Charging Station SHALL send a SecurityEventNotificationRequest message to the CSMS with the security event InvalidFirmwareSignature (See part 2 appendices for the full list of security events).	
L01.FR.04	When the Charging Station has successfully downloaded the new firmware	The signature SHALL be validated, by calculating the signature over the entire firmware file using the RSA-PSS or ECSchnorr algorithm for signing, and the SHA256 algorithm for calculating hash values.	
L01.FR.05	L01.FR.04 AND (*installDateTime* is not set OR current time >= *installDateTime*)	The Charging Station SHALL install the new firmware as soon as it is able to.	
L01.FR.06	L01.FR.05 AND The Charging Station has ongoing transactions AND When it is not possible to continue charging during installation of firmware	The Charging Station SHALL wait until all transactions have ended, before commencing installation.	
L01.FR.07	L01.FR.06 AND configuration variable `AllowNewSessionsPendingFirmwareUpdate` is *false* or does not exist	The Charging Station SHALL set all connectors that are not in use to UNAVAILABLE while the Charging Station waits for the ongoing transactions to end. Until the firmware is installed, any connector that becomes available SHALL be set to UNAVAILABLE.	
L01.FR.08		It is RECOMMENDED that the firmware is sent encrypted to the Charging Station. This can either be done by using a secure protocol (such as HTTPS, SFTP, or FTPS) to send the firmware, or by encrypting the firmware itself before sending it.	
L01.FR.09		Firmware updates SHALL be digitally protected to ensure authenticity and to provide proof of origin.	This protection is achieved by applying a digital signature over the hash value of the firmware image. Ideally, this signature is already computed by the manufacturer. This way proof of origin of the firmware image can be tracked back to the original author of the firmware.
L01.FR.10		Every FirmwareStatusNotificationRequest sent for a firmware update SHALL contain the same requestId as the UpdateFirmwareRequest that started this firmware update.	
L01.FR.11		For security purposes the CSMS SHALL include the Firmware Signing certificate (see Keys used in OCPP) in the UpdateFirmwareRequest.	
L01.FR.12		For verifying the certificate (see Certificate Hierarchy) use the rules for X.509 certificates [19]. The Charging Station MUST verify the file's digital signature using the Firmware Signing certificate.	
L01.FR.13	When the Charging Station enters the Download Scheduled state.	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status DownloadScheduled.	For example when it is busy with installing another firmware or it is busy Charging.
L01.FR.14	When the Charging Station enters the Download Paused state.	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status DownloadPaused.	For example when the Charging Station has tasks with higher priorities.

ID	Precondition	Requirement definition	Note
L01.FR.15	When a Charging Station needs to reboot before installing the downloaded firmware.	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status InstallRebooting, before rebooting.	
L01.FR.16	L01.FR.04 AND When *installDateTime* is set to a time in the future	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status InstallScheduled and install the firmware at the specified installation time.	
L01.FR.20		The field *requestId* in FirmwareStatusNotificationRequest is mandatory, unless *status* = Idle.	
L01.FR.21	When the Charging Station receives an UpdateFirmwareRequest	The Charging Station SHALL validate the certificate before accepting the message.	
L01.FR.22	L01.FR.21 AND the certificate is invalid	The Charging Station SHALL respond with UpdateFirmwareResponse with status `InvalidCertificate`.	
L01.FR.23	When the Charging Station needs to reboot during a firmware update AND the bootloader is unable to send OCPP messages	The Charging Station MAY omit the FirmwareStatusNotificationRequest message with status Installing.	
L01.FR.24	When a Charging Station is installing new Firmware OR is going to install new Firmware, but has received an UpdateFirmware command to install it at a later time AND the Charging Station receives a new UpdateFirmwareRequest	The Charging Station SHOULD cancel the ongoing firmware update AND respond with status `AcceptedCanceled`.	The Charging Station SHOULD NOT first check if the new firmware file exists, this way the CSMS will be able to cancel an ongoing firmware update without starting a new one.
L01.FR.25	Charging Station receives a TriggerMessageRequest for `FirmwareStatusNotification` AND last sent FirmwareStatusNotificationRequest had *status* = Installed	Charging Station SHALL return a FirmwareStatusNotificationRequest with *status* = Idle.	
L01.FR.26	Charging Station receives a TriggerMessageRequest for `FirmwareStatusNotification` AND last sent FirmwareStatusNotificationRequest had NOT *status* Installed	Charging Station SHALL return a FirmwareStatusNotificationRequest with the last sent *status*.	
L01.FR.27	L01.FR.24 AND the Charging Station is unable to cancel the firmware installation	The Charging Station MAY respond with *status* = `Rejected`.	
L01.FR.28	After Charging Station has sent FirmwareStatusNotificationRequest with *status* = Installed	Charging Station SHOULD have activated the new firmware or do so immediately. This MAY involve an automatic reboot, but not necessarily so.	

L02 - Non-Secure Firmware Update

Table 194. L02 - Non-Secure Firmware Update

No.	Type	Description
1	**Name**	Non-Secure Firmware Update
2	**ID**	L02
	Functional block	L. Firmware Management
3	**Objective(s)**	Download and install a Non-Secure firmware update.
4	**Description**	Illustrate how a Charging Station processes a Non-Secure firmware update.

No.	Type	Description
	Actors	CSMS, Charging Station
	Scenario description	**1.** The CSMS sends an UpdateFirmwareRequest message that contains the location of the firmware, the time after which it should be retrieved, and information on how many times the Charging Station should retry downloading the firmware. **2.** The Charging station responds with an UpdateFirmwareResponse. **3.** The Charging station sends a FirmwareStatusNotificationRequest with status *Downloading*. **4.** The CSMS responds with a FirmwareStatusNotificationResponse. **5.** The Charging station sends a FirmwareStatusNotificationRequest with status *Downloaded*. **6.** The CSMS responds with a FirmwareStatusNotificationResponse. **7.** The Charging station sends a FirmwareStatusNotificationRequest with status *Installing*. **8.** The CSMS responds with a FirmwareStatusNotificationResponse. **9.** The Charging station sends a FirmwareStatusNotificationRequest with status *Installed*. **10.** The CSMS responds with a FirmwareStatusNotificationResponse.
	Alternative scenario(s)	L01 - Secure Firmware Update
5	**Prerequisite(s)**	The Charging Station Manufacturer provided a firmware update.
6	**Postcondition(s)**	**Successful postcondition:** Firmware update was successfully installed. **Failure postcondition:** Firmware update failed.

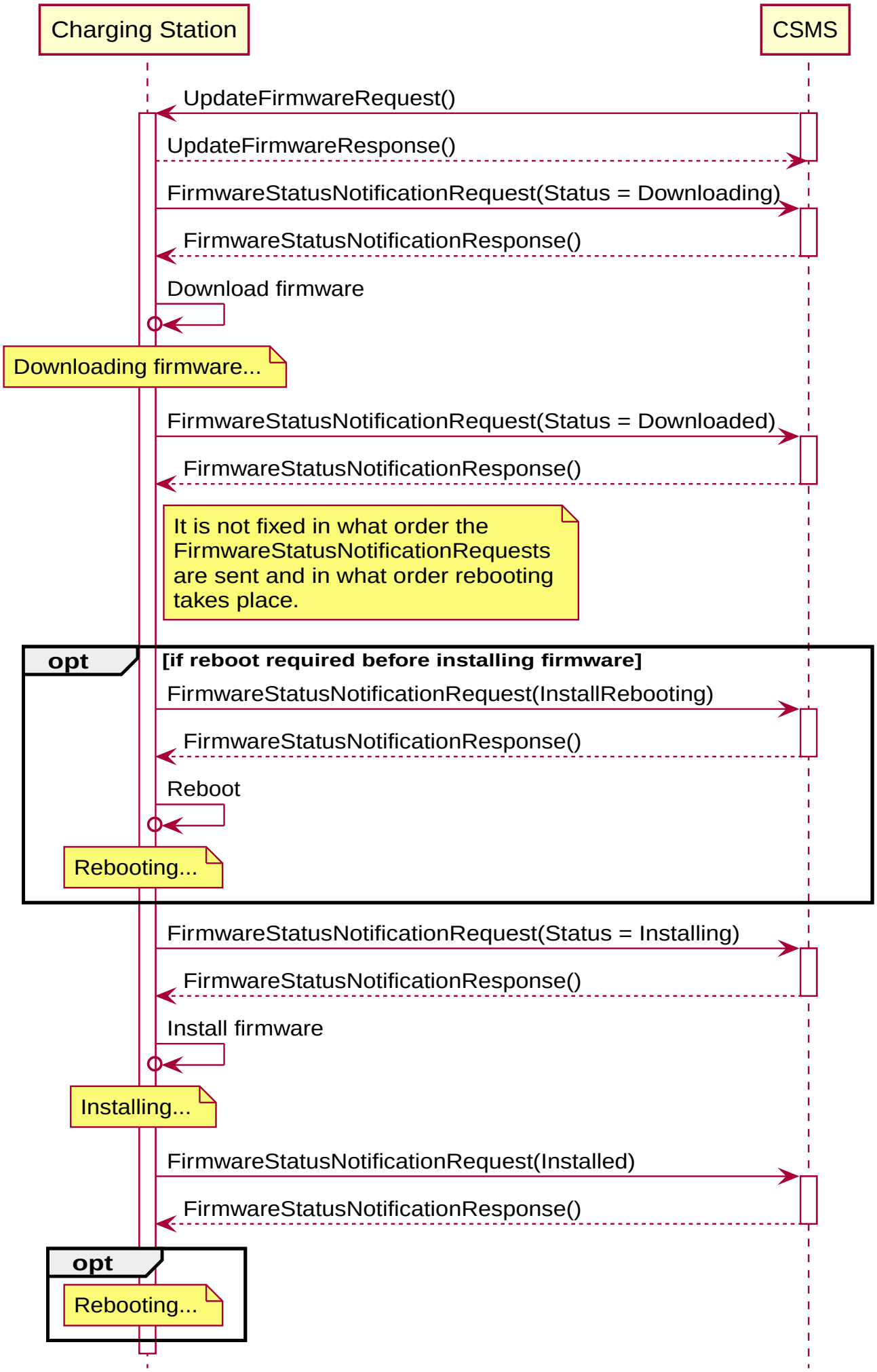
Charging Station
CSMS
UpdateFirmwareRequest()
UpdateFirmwareResponse()
FirmwareStatusNotificationRequest(Status = Downloading)
FirmwareStatusNotificationResponse()
Download firmware
Downloading firmware...
FirmwareStatusNotificationRequest(Status = Downloaded)
FirmwareStatusNotificationResponse()
It is not fixed in what order the FirmwareStatusNotificationRequests are sent and in what order rebooting takes place.
opt
[if reboot required before installing firmware]
FirmwareStatusNotificationRequest(InstallRebooting)
FirmwareStatusNotificationResponse()
Reboot
Rebooting...
FirmwareStatusNotificationRequest(Status = Installing)
FirmwareStatusNotificationResponse()
Install firmware
Installing...
FirmwareStatusNotificationRequest(Installed)
FirmwareStatusNotificationResponse()
opt
Rebooting...

Figure 118. Sequence diagram Non-Secure firmware upgrade

7	**Error handling**	n/a
8	**Remark(s)**	Measures SHOULD be taken to secure the firmware when it is stored on a server or workstation. When migrating to a new version of OCPP it is RECOMMENDED to install a fallback NetworkConnectionProfile with the new configuration. FTP needs to be able to use Passive FTP, to be able to transverse over as much different typologies as possible.

L02 - Non-Secure Firmware Update - Requirements

Table 195. L02 - Requirements

ID	Precondition	Requirement definition	Note
L02.FR.01	Whenever the Charging Station enters a new status in the firmware update process.	The Charging Station SHALL send a FirmwareStatusNotificationRequest message to the CSMS with this new status.	
L02.FR.02	When the Charging Station has successfully downloaded the new firmware AND (*installDateTime* is not set OR current time >= *installDateTime*)	The Charging Station SHALL install the new firmware as soon as it is able to.	
L02.FR.03	L02.FR.02 AND The Charging Station has ongoing transactions AND When it is not possible to continue charging during installation of firmware	The Charging Station SHALL wait until all transactions have ended, before commencing installation.	
L02.FR.04	L02.FR.03 AND configuration variable `AllowNewSessionsPendingFirmwareUpdate` is *false* or does not exist	The Charging Station SHALL set all connectors that are not in use to UNAVAILABLE while the Charging Station waits for the ongoing transactions to end. Until the firmware is installed, any connector that becomes available SHALL be set to UNAVAILABLE.	
L02.FR.05		It is RECOMMENDED that the firmware is sent encrypted to the Charging Station. This can either be done by using a secure protocol (such as HTTPS, SFTP, or FTPS) to send the firmware, or by encrypting the firmware itself before sending it.	
L02.FR.06		Every FirmwareStatusNotificationRequest sent for a firmware update SHALL contain the same requestId as the UpdateFirmwareRequest that started this firmware update.	
L02.FR.07	When the Charging Station enters the Download Scheduled state.	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status DownloadScheduled.	For example when it is busy with installing another firmware or it is busy Charging.
L02.FR.08	When the Charging Station enters the Download Paused state.	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status DownloadPaused.	For example when the Charging Station has tasks with higher priorities.
L02.FR.09	When a Charging Station needs to reboot before installing the downloaded firmware.	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status InstallRebooting, before rebooting.	
L02.FR.10	When the Charging Station has successfully downloaded the new firmware AND *installDateTime* is set to time in the future	The Charging Station SHALL send a FirmwareStatusNotificationRequest with status InstallScheduled and install the firmware at the specified installation time.	

ID	Precondition	Requirement definition	Note
L02.FR.14		The field *requestId* in FirmwareStatusNotificationRequest is mandatory, unless *status* = `Idle`.	
L02.FR.15	When a Charging Station is installing new Firmware OR is going to install new Firmware, but has received an UpdateFirmware command to install it at a later time AND the Charging Station receives a new UpdateFirmwareRequest	The Charging Station SHOULD cancel the ongoing firmware update AND respond with status *AcceptedCanceled*.	The Charging Station SHOULD NOT first check if the new firmware file exists, this way the CSMS will be able to cancel an ongoing firmware update without starting a new one.
L02.FR.16	Charging Station receives a TriggerMessageRequest for `FirmwareStatusNotification` AND last sent FirmwareStatusNotificationRequest had *status* = `Installed`	Charging Station SHALL return a FirmwareStatusNotificationRequest with *status* = `Idle`.	
L02.FR.17	Charging Station receives a TriggerMessageRequest for `FirmwareStatusNotification` AND last sent FirmwareStatusNotificationRequest had NOT *status* `Installed`	Charging Station SHALL return a FirmwareStatusNotificationRequest with the last sent *status*.	
L02.FR.18	L02.FR.15 AND the Charging Station is unable to cancel the firmware installation	The Charging Station MAY respond with *status* = `Rejected`.	

L03 - Publish Firmware file on Local Controller

Table 196. L03 - Publish Firmware file on Local Controller

No.	Type	Description
1	**Name**	Publish Firmware file on Local Controller.
2	**ID**	L03
	Functional block	L. FirmwareManagement
3	**Objective(s)**	To allow Charging Stations to download a firmware update directly from the Local Controller.
4	**Description**	The Local Controller downloads and publishes a firmware update at the specified URL. This allows the CSMS to send UpdateFirmwareRequests with the URI pointing to the Local Controller, to any Charging Station connected to the Local Controller. This allows the site to save bandwidth and data on the WAN interface.
	Actors	Local Controller, CSMS
	Scenario description	**1.** The CSMS sends a PublishFirmwareRequest to instruct the Local Controller to download and publish the firmware, including an MD5 checksum of the firmware file. **2.** Upon receipt of PublishFirmwareRequest, the Local Controller responds with PublishFirmwareResponse. **3.** The Local Controller starts downloading the firmware. **4.** The Local Controller verifies the MD5 checksum. **5.** The Local Controller publishes the firmware file at the URI(s) stated in PublishFirmwareStatusNotificationRequest. **6.** The CSMS instructs Charging Stations to update their firmware, as described in Use Case L01 - Secure Firmware Update
5	**Prerequisite(s)**	n/a

No.	Type	Description
6	**Postcondition(s)**	**Successful postcondition:** The firmware is successfully published by the Local Controller. **Failure postcondition:** The Local Controller could not download the firmware file, and has sent the *DownloadFailed* status. The Local Controller could not verify the MD5 checksum, and has sent the *InvalidChecksum* status. The Local Controller could not publish the firmware file, and has sent the *PublishFailed* status.

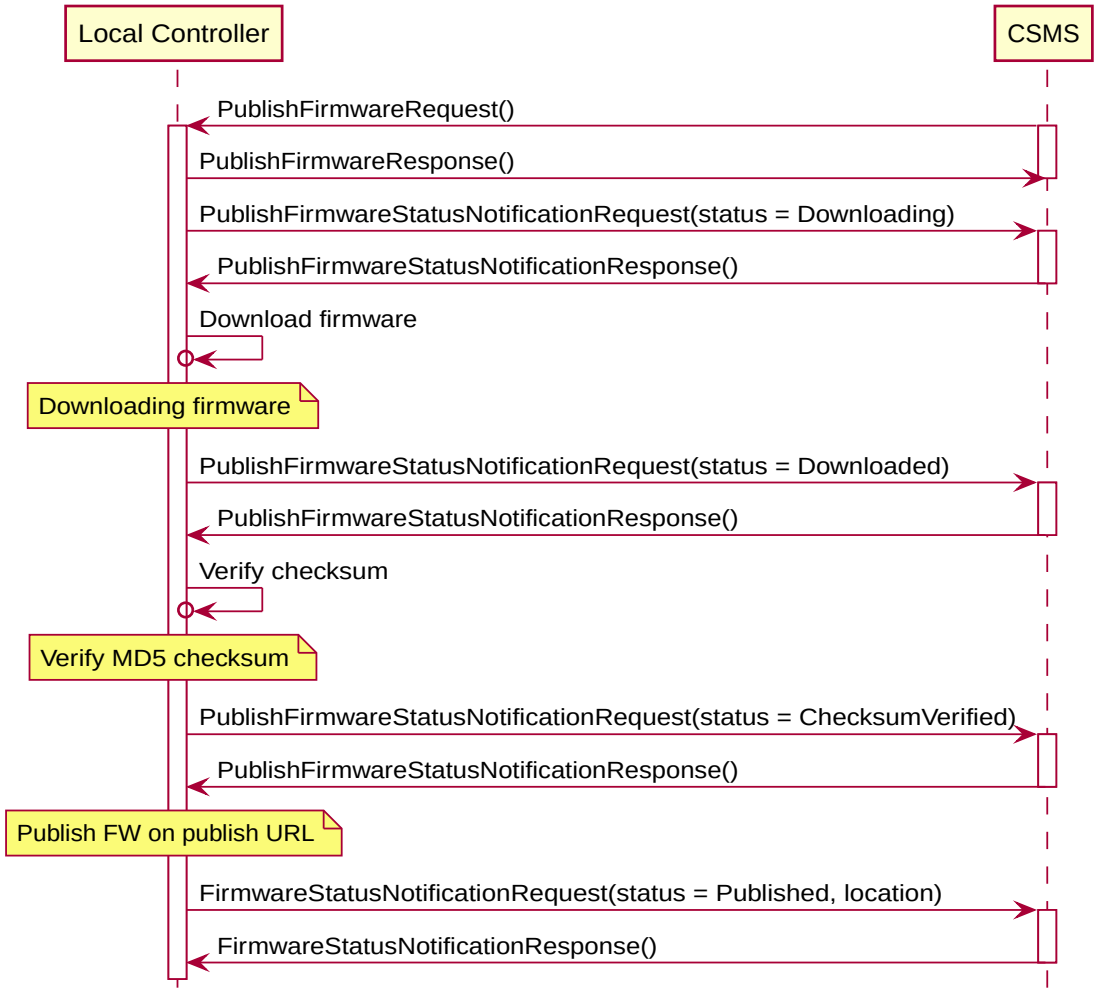

Figure 119. Sequence Diagram: showing publishing of firmware (happy flow)

7	**Error handling**	n/a
8	**Remark(s)**	For information about MD5 checksum see RFC-1321 [RFC1321].

L03 - Publish Firmware file on Local Controller - Requirements

Table 197. L03 - Requirements

ID	Precondition	Requirement definition
L03.FR.01		Whenever the Local Controller enters a new status in the publishing process, it SHALL send a PublishFirmwareStatusNotificationRequest message to the CSMS.
L03.FR.02		The MD5 checksum SHALL be calculated over the entire firmware file.
L03.FR.03		The Local Controller SHALL publish the firmware file using all its supported protocols (e.g. HTTP, HTTPS, and FTP)

ID	Precondition	Requirement definition
L03.FR.04		The Local Controller SHALL set URI's for all supported protocols (e.g. HTTP, HTTPS, and FTP) in the *location* field of the PublishFirmwareStatusNotificationRequest message with status *Published*.
L03.FR.05	Upon receipt of a PublishFirmwareRequest message.	The Local Controller SHALL respond with a PublishFirmwareResponse message, indicating whether it has accepted the request.
L03.FR.06	If the Local Controller cannot download the firmware file.	The Local Controller SHALL send a PublishFirmwareStatusNotificationRequest with status *DownloadFailed*.
L03.FR.07	If the Local Controller cannot verify the MD5 checksum.	The Local Controller SHALL send a PublishFirmwareStatusNotificationRequest with status *InvalidChecksum*.
L03.FR.08	If the Local Controller cannot publish the firmware file.	The Local Controller SHALL send a PublishFirmwareStatusNotificationRequest with status *PublishFailed*.
L03.FR.09	After successfully publishing the firmware file.	The Local Controller SHALL send a PublishFirmwareStatusNotificationRequest with status *Published*.
L03.FR.10	Charging Station receives a TriggerMessageRequest for `PublishFirmwareStatusNotification` AND last sent PublishFirmwareStatusNotificationRequest had *status* = `Published`	Charging Station SHALL return a PublishFirmwareStatusNotificationRequest with *status* = `Idle`.
L03.FR.11	Charging Station receives a TriggerMessageRequest for `PublishFirmwareStatusNotification` AND last sent PublishFirmwareStatusNotificationRequest had NOT *status* `Published`	Charging Station SHALL return a PublishFirmwareStatusNotificationRequest with the last sent *status*.

L04 - Unpublish Firmware file on Local Controller

Table 198. L04 - Unpublish Firmware file on Local Controller

No.	Type	Description
1	**Name**	Unpublish Firmware file on Local Controller.
2	**ID**	L04
	Functional block	L. FirmwareManagement
3	**Objective(s)**	Stop the Local Controller from publishing a firmware update to Charging Stations.
4	**Description**	Stop serving a firmware update to connected Charging Stations.
	Actors	Local Controller, CSMS
	Scenario description	1. The CSMS sends an UnpublishFirmwareRequest to instruct the local controller to unpublish the firmware. 2. The Local Controller unpublishes the firmware. 3. The local Controller responds with an UnpublishFirmwareResponse.
5	**Prerequisite(s)**	A firmware successfully published by the Local Controller.
6	**Postcondition(s)**	**Successful postcondition:** Firmware file no longer published. **Failure postcondition:** n/a

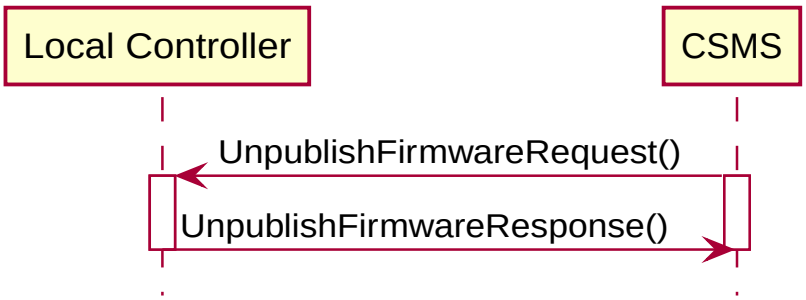

Figure 120. Sequence Diagram: Unpublishing a firmware file

7	**Error handling**	n/a
8	**Remark(s)**	The CSMS uses a MD5 checksum over the entire firmware file as a unique identifier to indicate which firmware file needs to be unpublished.

L04 - Unpublish Firmware file on Local Controller - Requirements

Table 199. L04 - Requirements

ID	Precondition	Requirement definition
L04.FR.01	If the Local Controller receives an UnpublishFirmwareRequest message AND There is no ongoing download.	The firmware file SHALL be unpublished.
L04.FR.02	After successfully unpublishing the firmware file.	The local controller SHALL send an UnpublishFirmwareResponse message with status *Unpublished*.
L04.FR.03	If the Local Controller receives an UnpublishFirmwareRequest message AND There is no published file.	The Local Controller SHALL send an UnpublishFirmwareResponse message with status *NoFirmware*.
L04.FR.04	If the Local Controller receives an UnpublishFirmwareRequest message AND If a Charging Station is downloading the firmware file.	The Local Controller SHALL respond with the *Downloading* status AND **not** unpublish the firmware file.