

---

# Autocharge

Automatic charging start and authorization of electric vehicles

---

## What is Autocharge?

AutoCharge is a mechanism to authorize electrical vehicle for charging based on a vehicle identifier. For an EV driver it would be as simple as plugging in his/her car to charger and let charger to do authorization automatically to allow (or not) for charging to start.

## How it works for an EV driver

- A driver arrives at a charging station and plugs in
- Charging starts immediately and the driver can walk away
- The payment is processed in the background via his/her regular contract with the provider

## How it works from a technical perspective

Autocharge is technically very simple. To implement it you need only a couple of things:

1. Ability to read something uniquely identifying the vehicle when the connector is plugged in. There is no agreement yet on a unified vehicle id, but a lot of cars have a MAC (Media Access Control) address assigned to it, just like any device connected to the Internet. NOTE: At the moment only CCS protocol is providing MAC address during communication between vehicle and charger.
2. An OCPP enabled charger. Autocharge is using OCPP to communicate with Central System, in particular Authorize command to send MAC address to Central System. Every version of OCPP from 1.5 and on is capable to implement it. In the coming OCPP versions there will be a dedicated field or type for vehicle id
3. Logic implemented in back-end system (OCPP Central system) to authorize based on MAC address of a vehicle.

That's it!

Charger manufacturers should take care of reading MAC address of a vehicle when CCS connector is plugged in and then sending OCPP Authorize request with this respective MAC address as idTag. The messages must have the prefix idTag with "VID" in this case, so this type of request could be distinguished from other types (e.g. authorizing with RFID card). The VID has a maximum of 8 bytes but is typically 6 or 8 bytes

Back-end system providers should implement appropriate logic in his OCPP Central System to interpret MAC address from idTag and send Authorize response back to the Charge Point. It is up to back-end system provider to implement as sophisticated logic for authorization as desired (e.g. assigning many vehicles to one user account, combining authorization modes or select preferred one based on various settings, etc)

## Key benefits

- Highly user friendly interaction
- Very simple to implement
- No major back-office changes to OCPP based charging networks

- Works with new and old vehicles (already on the road)
- Ability to index vehicle id's automatically at the first charging session (new and old)

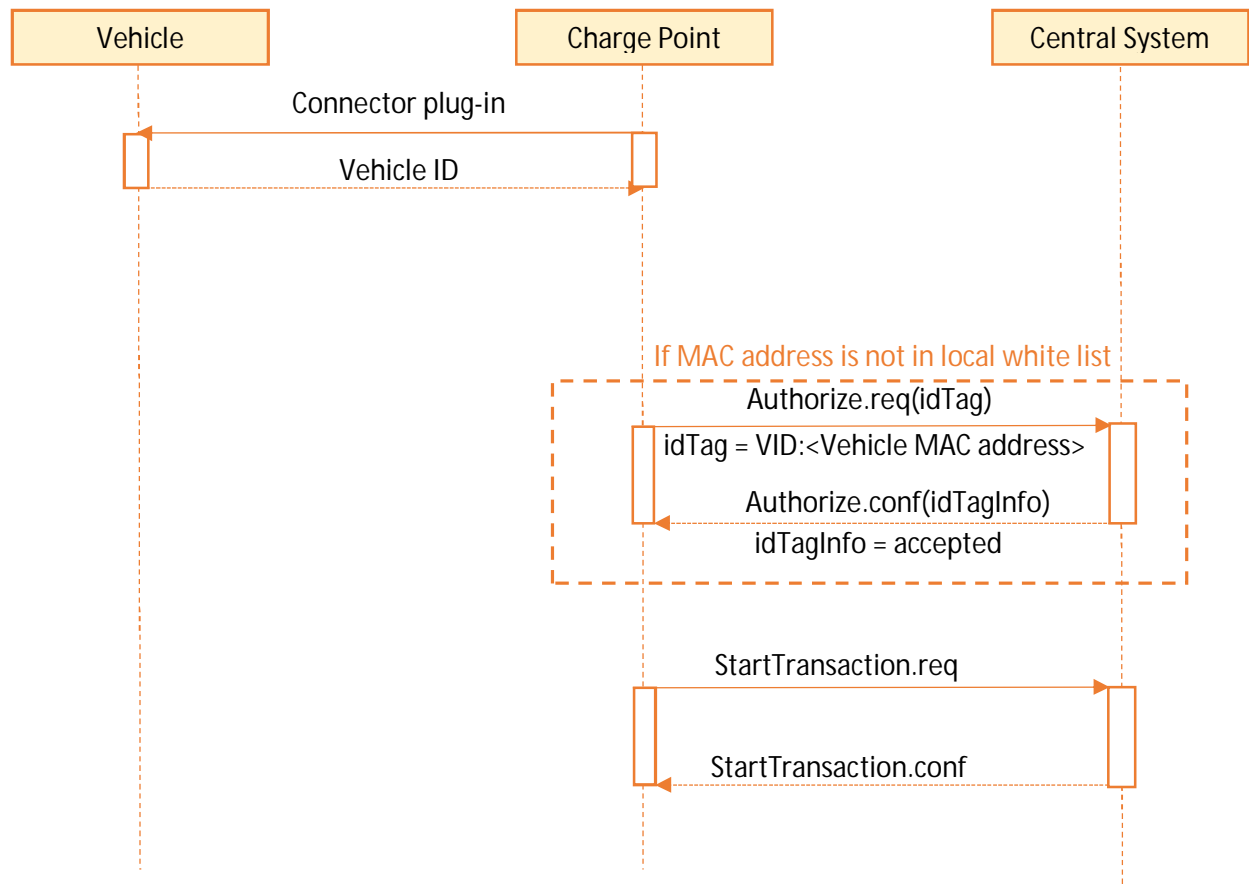
## It is so simple, are there any drawbacks?

Autocharge is intended to be a simple and fast way to realize a very user friendly operation. Probably there will be some limitations going forward. At the moment Autocharge will only work with CCS based vehicles, however CHAdeMO could also easily include a vehicle ID or MAC address in the communication.

It is definitely more secure than RFID, because you couldn't that easily copy or simulate MAC address while a RFID card is very easy to copy. Should any misuse happen then it may be detected after some time by the back-office of the operator, camera's or driver reports and the access can be denied. The likelihood of this scenario probably does not outweigh the benefits of having a fast introduction of such a driver friendly feature.

## Schema

Please see example of how Autocharge implementation could work in diagram of OCPP commands.



## How it works together with traditional authorization methods

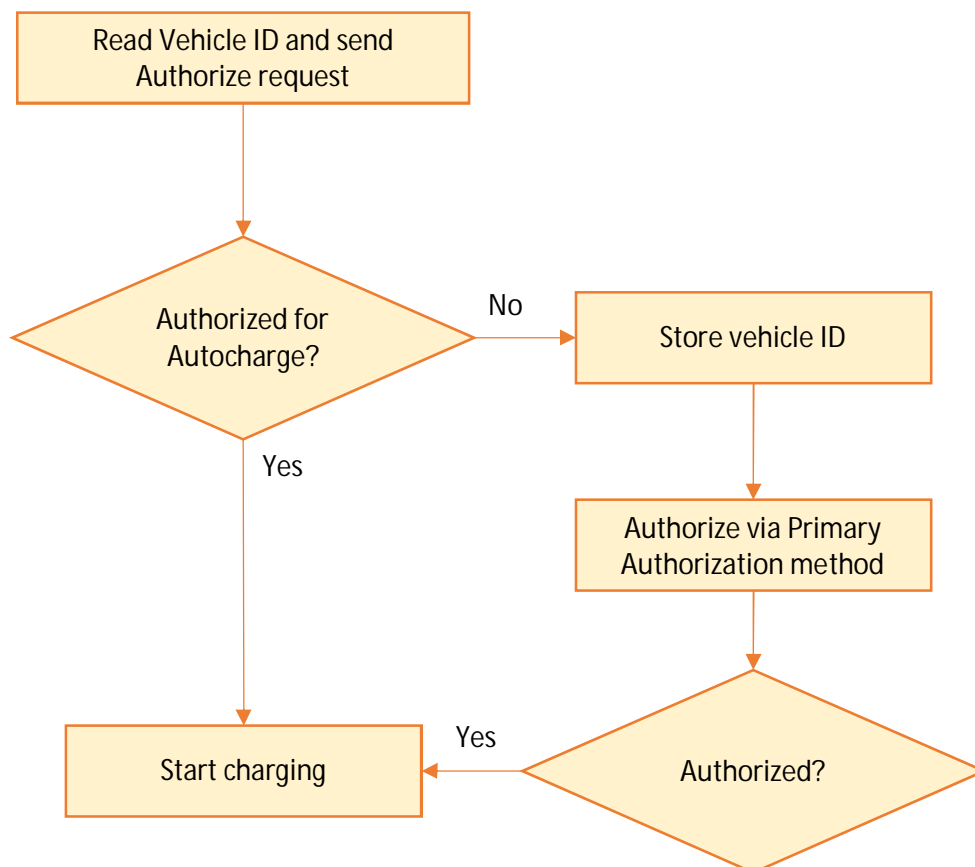
There are 2 main authorization methods used at the moment in charging:

1. Via RFID card reader built in a charger
2. Remote authorization, when user is authorized via phone app, SMS code, QR code scanning, etc.  
In other words via different channel than charger communication channel.

In case of Autocharge there should be always another (primary or initial) authorization method, namely one of the above. If authorization is not successful via Vehicle ID, charger should not indicate that authorization is failed, but wait for another authorization method. Otherwise it would result in bad user experience: authorization failure message might be displayed every time driver plugs in connector into a car.

### First time authorization

If a driver plugs in his vehicle for the first time, its vehicle ID might not be known by central system. In this case Vehicle ID should be stored by central system, so it can be associated with user account later:



As you see above, vehicle ID is stored by central system and in case of successful authorization via another method and successful charge session, charger operator could contact user to ask if he would like to associate vehicle ID with his account and enable Autocharge for future charge sessions.

OCPP protocol doesn't have command which could provide linking of vehicle ID to existing user account, so it should be done via other communication channel, e.g. web application, phone application, by phone with service representative, etc.

## How to stop charging started with Autocharge

To stop a charge session initiated by Autocharge any allowed method could be used as long as it is supported and properly implemented in the Charge Point and Central System. E.g. stop by a vehicle, remote stop by the user, local (Authorized or not, depending on settings and use case) stop by a user, etc.