Appendix [Technical Specifications and IT Security]

Technical requirement for charging infrastructures:
AC charging:
Single-phase and three-phase AC charging (up to 43kW):
The charging station is equipped with one or more Type 2 charging points. The charging station is capable of single-phase AC charging at up to 7.4kW (max.) and three-phase AC charging at up to 43kW (max.). The charging station varies its output according to the vehicle's charging capacity.
Single-phase AC charging (up to 7.3kW):
The charging station is equipped with a Type 2 charging point16, which is capable of single-phase AC charging at up to 3.7kW.

DC charging:
Combined Charging System:
The Combined Charging System (CCS) integrates single-phase and fast three-phase AC charging, DC home charging and ultra-fast DC charging at public access charging stations within one vehicle inlet. In Europe the connector, called "Combo 2", is based on the Type 2 AC connector and on the combo 2 connector (see Configuration FF of the IEC 62196-3) for high-performance DC charging.

CHAdeMO:
The CHAdeMO standard (see ISO/IEC 61851-23 and 61851-24) also supports fast DC charging. For charging the vehicle based on DC voltage CHAdeMO requires special connectors and plugs for electric vehicles and charging stations.

Certification of charging infrastructures:
To ensure that the charging infrastructure can be used safely it must be certified according to the requirements of current standards and norms and in line with the development of charging technology concepts. The operator or the manufacturer should ensure electrical safety and compliance with the standards: CE certification, compliance with the EMC directives, DIN SPEC 70121 and IEC 61439-7.
In addition, DC charging stations and charging systems should meet the requirements of the following standards: IEC 61851-23 (general requirements for DC charging stations), EIC 62196-3 (definition of DC charging connections using the Combi 1 (USA) and Combo 2 (Europe) connectors) and DIN SPEC 70121 (station to vehicle communication for DC charging, based on ISO/IEC 15118) and the ISO/IEC norm 15118 for the certificate-based communication between the electric vehicle, the charging station and the IT-system.

Requirements for charging station management and/or customer management and/or POI-data-management systems:

Interface between the charging station and the charging station management system:
The charging stations must be capable of communicating bidirectionally with the back-end system. Hubject does not define any specification regarding protocols for the communication between charging station management system and charging station.

Interface between the charging station management system and the Hubject system:
The charging station management system and the Hubject system communicate via defined interfaces based on web services, see **Appendix [OICP]**.

Compulsory requirements:
a) Remote activation and remote termination of charging sessions, as well as activation and termination of charging session using other authentication methods
b) Transfer of billing data (delivery notice / Charge Detail Record)
c) Transfer of static charging station location details (Point-of-Interest-Information)
d) Transfer of dynamic charging point status information (Point-of-Interest-Information)

Interface between the customer management system and the Hubject system:
The customer management system and Hubject's backend system communicate via defined interfaces based on web services, see **Appendix [OICP]**.

Compulsory requirements:
a) Remote activation and remote termination of charging sessions, as well as activation and termination of charging session using other authentication methods
b) Receiving of billing data (delivery notice / Charge Detail Record)
c) Receiving of location details of charging stations (Point-of-Interest-Information)

Interface between the POI-data management system and the Hubject system:
The POI-data management system and Hubject's backend system communicate via defined interfaces based on web services, see **Appendix [OICP]**.

Compulsory requirements:
a) Receiving of location details of charging stations (Point-of-Interest-Information)

Requirements for the IT security between charging station management systems and the Hubject system, as well as between customer management systems and/or POI-data management systems and the Hubject system

The Platform is accessed by Partners via the charging station management system and the customer management system as well as the POI-data management system.
The communication between them uses standard internet infrastructure. Thus the connections need to be secured to achieve the following general goals of information security:

- Confidentiality – messages can only be read by an intended recipient.
- Integrity – altering of messages during transmission (deliberately or by technical errors) must be detected.
- Authenticity – messages must be attributable to a unique sender. The sender must not be able to repudiate the transmission of a message.

Incoming connections from the Partner backend are sent via the internet to a load balancer node of the Platform which acts as a reverse proxy. The connection is distributed to a cluster of service processing nodes. The connection has to pass a 2-layered firewall when entering the network of the Platform.
Both the reverse proxy and the firewall provide access control using white lists which grant access only to specific IP addresses. The firewall at the network and transport layer is restricted to allowed source/destination IPs and ports. The proxy at the application layer is restricted to certain URLs.
Outgoing connections from the Platform are sent directly to the Partner backend systems but have to pass the firewall as well.
The web services are transmitted using the HTTP protocol. The SSL/TLS secured HTTPS variant encapsulates HTTP.

The SSL tunnel guarantees the above goals of information security: confidentiality via encryption, integrity via signed checksums and authenticity via authentication using digital signatures and certificates.
With HTTPS strong server and client authentication using certificates will be used to authenticate the actual connection used for each service call.
The reverse proxy / load balancer handles the central HTTPS encryption and authentication of all incoming connections to the Platform. This includes the requests for the portal which is accessed by users with their web browsers.
No changes to the Platform are required to add a new Partner.