

Advies aanbestedingseisen laadinfrastructuur elektrische bussen voor DOVA

Laadinfrastructuur algemeen

- Algemene aanbevelingen zijn te vinden in de [NKL Basisset DC-laden](#).
- Voor de communicatie tussen voertuig en laadinfrastructuur wordt het laadprotocol ISO 15118 gebruikt.

Fysieke veiligheid

- Zorg voor goede aanrijdbeveiliging, ook van de transformator(en) en de omvormerkast(en).
- Geef de chauffeurs en andere gebruikers goede instructies.
- Zorg dat de installatieverantwoordelijkheid goed is geregeld.

Cybersecurity

- Bij voorkeur wordt gevraagd dat de laadinfrastructuur voldoet aan de [ENCS-requirements](#). N.B. het kost de aanbieder ongeveer €30k om d.m.v. een onafhankelijke test aan te tonen dat hij aan deze requirements voldoet.
- Gebruik voor de communicatie tussen oplaadpunt en back-end het Open Charge Point Protocol (OCPP), minimaal versie 1.6 met cybersecuritycertificaat maar bij voorkeur versie 2.0.1.
- Zorg dat alle communicatie beveiligd is door encryptie om inbreuk op de data door ongeautoriseerde derden te voorkomen.
- Zorg voor beveiliging van digitale toegang tot de laadinfrastructuur, zodat bijvoorbeeld monteurs niet zonder wachtwoord kunnen inloggen.
- Vraag aan de 'Charge Point Operator' of deze een melding krijgt als iemand ongeautoriseerd fysieke toegang tot de laadinfrastructuur probeert te krijgen.
- Vraag of de backoffice bij de Charge Point Operator ISO 27001 gecertificeerd is.
- Informeer hoe wordt gecontroleerd dat alleen geverifieerde software (voorzien van de juiste certificaten en digitale handtekeningen) op het oplaadpunt geïnstalleerd wordt.
- Vraag, als er bij een pantograafopstelling een wifiverbinding wordt gebruikt, hoe deze beveiligd is.
- Indien de laadinfrastructuur gekoppeld is aan een bufferbatterij en/of aan een energiemanagementsysteem en/of derden (bijv. een energieleverancier) moeten ook deze systemen en interfaces veilig zijn. Cybersecurity betreft de gehele keten.