

Back End

App

Microcontroller/Vehicle

- root certificate
- back end certificate & private key
- subscription certificate & private key

- root certificate
- app certificate & private key

- root certificate
- vehicle certificate & private key

subscription request
(vehicle ID, timestamp)

- create payload
(vehicle ID, timestamp, ...)
- hash and sign payload with
private subscription key

subscription
(payload, signature,
subscription certificate)

establish secure connection
via BLE using TLS

subscription

- verify subscription
certificate
- verify signature

→ secure connection
→ Bluetooth connection

