



**Driver**

**Smartphone application**

**Car with smartcard**

1. Sends car command

2.1 AES key exchange

2.2: Succes

3. Create msg =  
command || bookingID  
|| timestamp

4. Encrypt msg  
with AES key

5. Send msg

6. Decrypt msg with  
AES key recieved in  
Step 2

if timestamp.valid()

if bookingID == activeBooking.id

7. Execute  
command

