Scenario : You are to demonstrate the ability to generate a PoP CWT (pronounced "cot"). Where PoP is Proof-of-Possession, CWT is CBOR Web Token, and CBOR is Concise Binary Object Representation.

We are using the PoP CWT to demonstrate an approach to authorization (Az) in a vehicle network. In this lab we'll assume that a client can be authorized to one or more of 6 functions (called "func1", "func2", ... "func6").

A CWT with proof-of-possession is a lightweight approach to authorization.

Exercise 1 : Create a program that writes "pop.cwt" to a file, where the CWT is:

- for an ECU that is authorized to use "func4" and "func6".
- signed by the OEM.
- 'cnf' field is the ECUs public key for signing.

NOTE: you can use code from 'classroom' folder (key generation, etc.)
NOTE: your program should check that the CWT is valid.

Exercise 2 : Demonstrate the ability to move the CWT over the CANBUS. You are free to use tools provided by 'can-utils'.

Exercise 3 : [EXTRA CREDIT] Demonstrate the ability for the recipient of the CWT to challenge the ECU to sign a nonce provided by the recipient.