1.The system is implemented in a **Linux simulation environment** and not on a real automotive microcontroller or ECU hardware.

*2. **TCP socket communication** is used instead of real in-vehicle communication protocols such as CAN, LIN, or FlexRay.
response:

We are going to implement CAN protocol (Next step)
3. The **True Random Number Generator** is based on Linux (`/dev/urandom`), not on a dedicated hardware TRNG.

Response:

If we choose a micro-controller(infinieoun) we can implement in that based TRNG.

4. The project supports **only a single transponder-client connection** at a time.

5. **No protection against replay attacks beyond timeouts** (no counters or nonces stored across sessions).

6. No secure key provisioning or key update mechanism is implemented.

7. **No secure storage mechanism** is used for secret keys (e.g., HSM or secure element).

Both values
8. No handling of power loss or reset during authentication