Engine ECU – Transponder ECU Authentication Design

Transponder ECU is considered as a client, while the Engine ECU acts as the authenticator. The authentication mechanism is implemented in two levels to demonstrate basic and advanced challenge–response behavior using AES encryption.

Level 1: Basic Challenge–Response Authentication

Overall Flow

1. Transponder ECU sends a *start* signal to the Engine ECU.
2. Engine ECU receives the start signal, generates a random number (challenge), and computes its AES-encrypted value.
3. Transponder ECU receives the random number, encrypts it using the same AES key, and sends the encrypted value back to the Engine ECU.
4. Engine ECU compares the received encrypted value with its own computed value and decides authentication success or failure.

Engine ECU – Level 1 Steps

- Wait for start signal from Transponder ECU.
- Generate a random 128-bit challenge.
- Encrypt the challenge using AES-128.
- Send the random challenge to the Transponder ECU.
- Receive encrypted response from Transponder ECU.
- Compare received value with expected AES result.
- Declare authentication success or failure.

Transponder ECU – Level 1 Steps

- Initiate authentication by sending start signal.
- Receive random challenge from Engine ECU.
- Encrypt the challenge using AES-128.
- Send encrypted value back to Engine ECU.

Level 2: Timed and Robust Authentication

Overall Flow

1. Transponder ECU sends a start signal (same as Level 1).

2 Engine ECU generates a random challenge, encrypts it using AES, and sends the random number to the Transponder ECU.

3 Engine ECU waits for a maximum of 4 seconds for a response.

4 If no response is received within 4 seconds, Engine ECU generates a new random challenge and repeats the process.

5 If total authentication time exceeds 20 seconds, authentication fails.

6 If a valid encrypted response is received within time, authentication succeeds.

Engine ECU – Level 2 Steps

- Record global authentication start time.
- Generate random challenge using TRNG.
- Encrypt challenge using AES-128.
- Send challenge to Transponder ECU.
- Wait up to 4 seconds for response.
- If response is missing, generate a new challenge.
- If response is received, validate encrypted value.
- Fail authentication if total time exceeds 20 seconds.
- Declare success or failure.

Transponder ECU – Level 2 Steps

- Send start signal to Engine ECU.
- Wait for random challenge.
- Encrypt received challenge using AES-128.
- Send encrypted response back within time limit.
- Authentication succeeds only if timing and encryption are valid.