Interaction with eSIM at Physical Layer

July 28, 2024

Introduction

- The activation of the ST4SIM200M eSIM complies with the ISO/IEC 7816-3:2006 standards.
- The ISO/IEC 7816-3:2006 standard provides information on interacting with eSIMs at the physical and data-link layers.
- When interacted via physical layer we get ATR(Answer to Reset) from eSIM.
- An Arduino UNO serves as a UART interface for the eSIM.

ST4SIM200M Pin Diagram

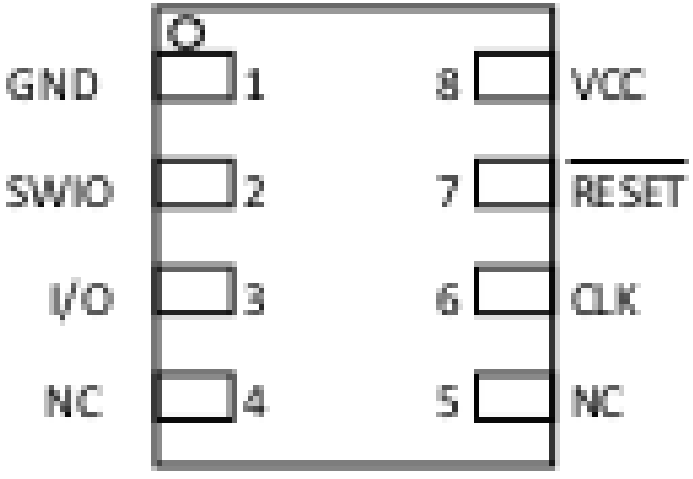


Figure: Pin Diagram

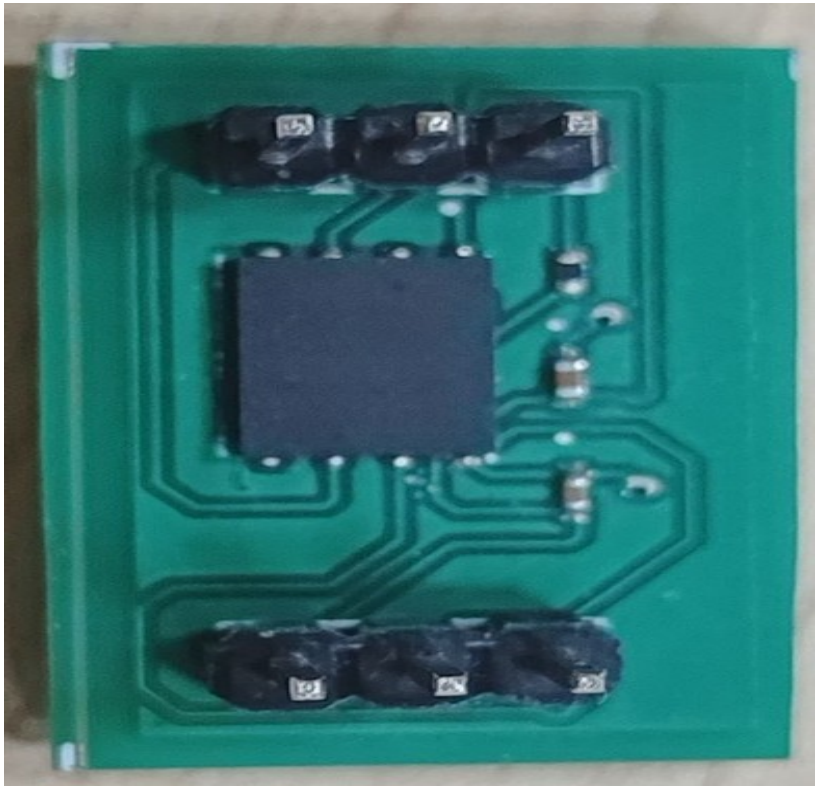


Figure: eUICC

eSIM Pin Inputs

Table 1:
Inputs

Pin No	Pin Description	Value
1	GND	ground
2	SWIO	No Connection
3	I/O	Information Exchange
4	NC	No Connection
5	NC	No Connection
6	CLK	2MHz frequency (40-60% duty cycle)
7	RESET	0V/5V
8	VCC	5V

eSIM Activation Process

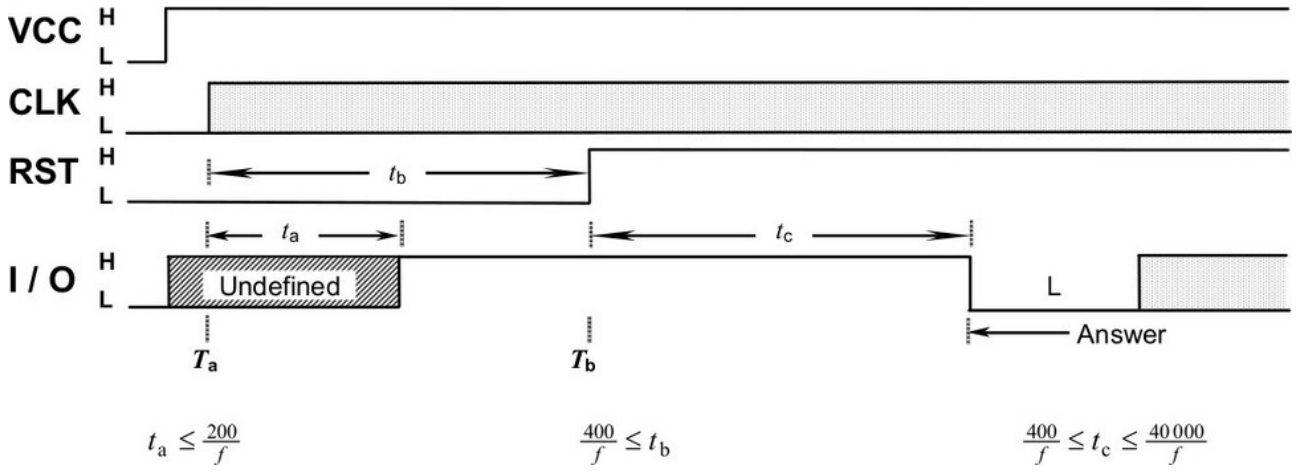


Figure 1: Activation and Cold Reset

Logic Analyser Output

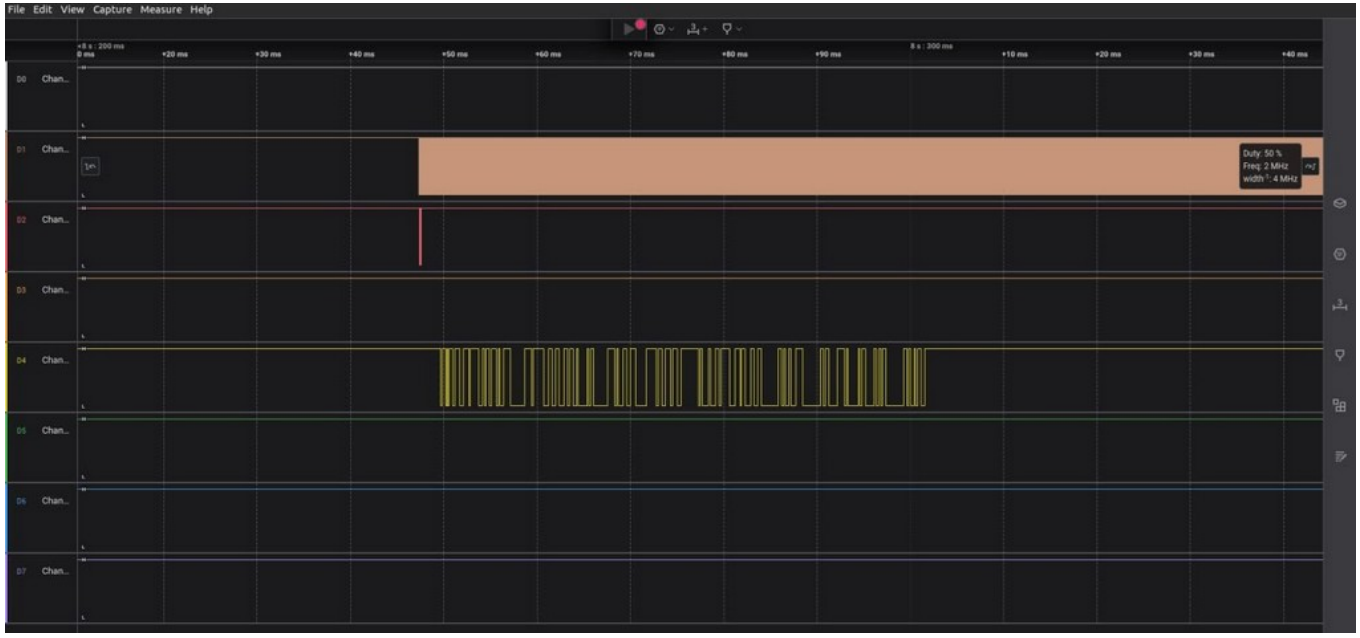


Figure 2: Activation and Cold Reset Response

Serial monitor response

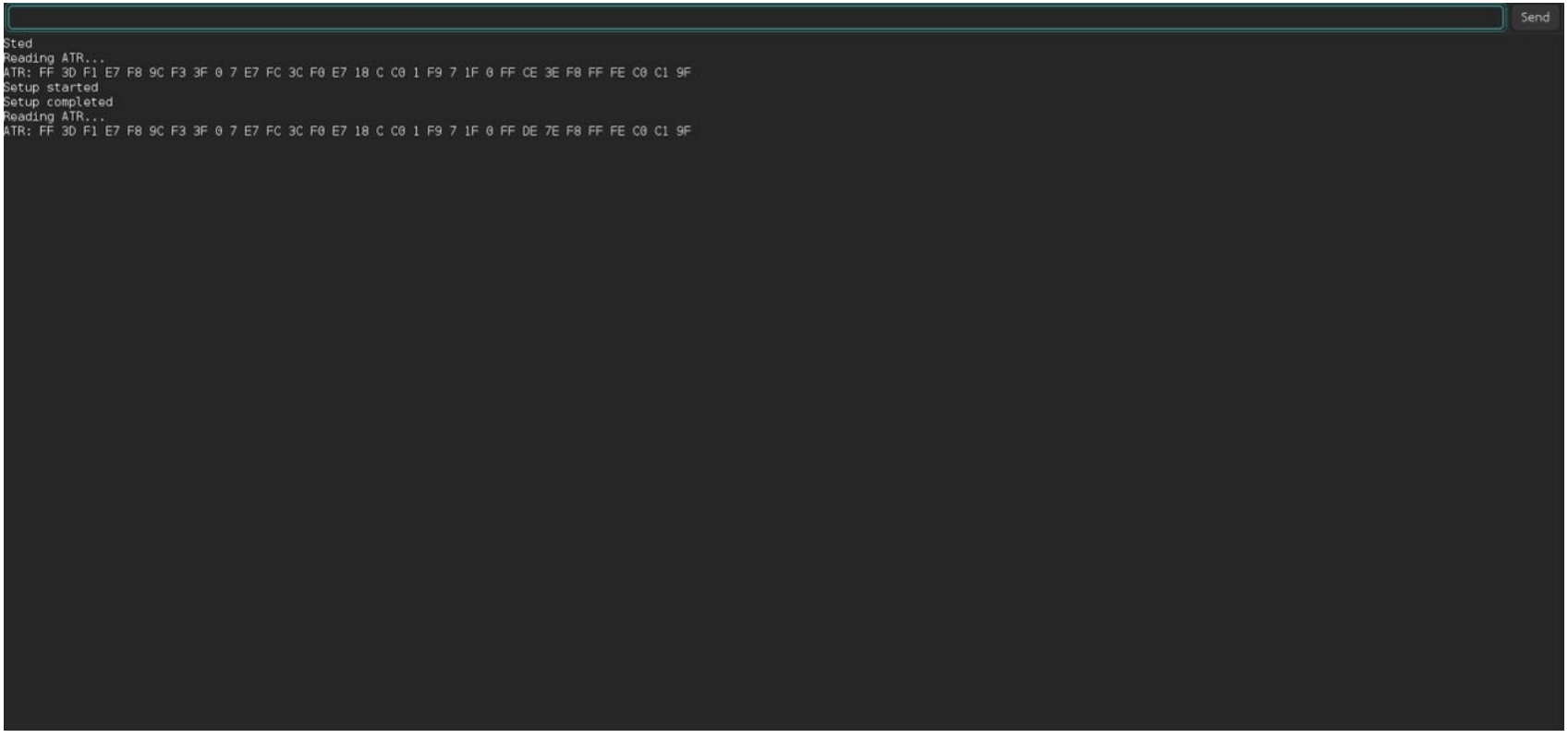
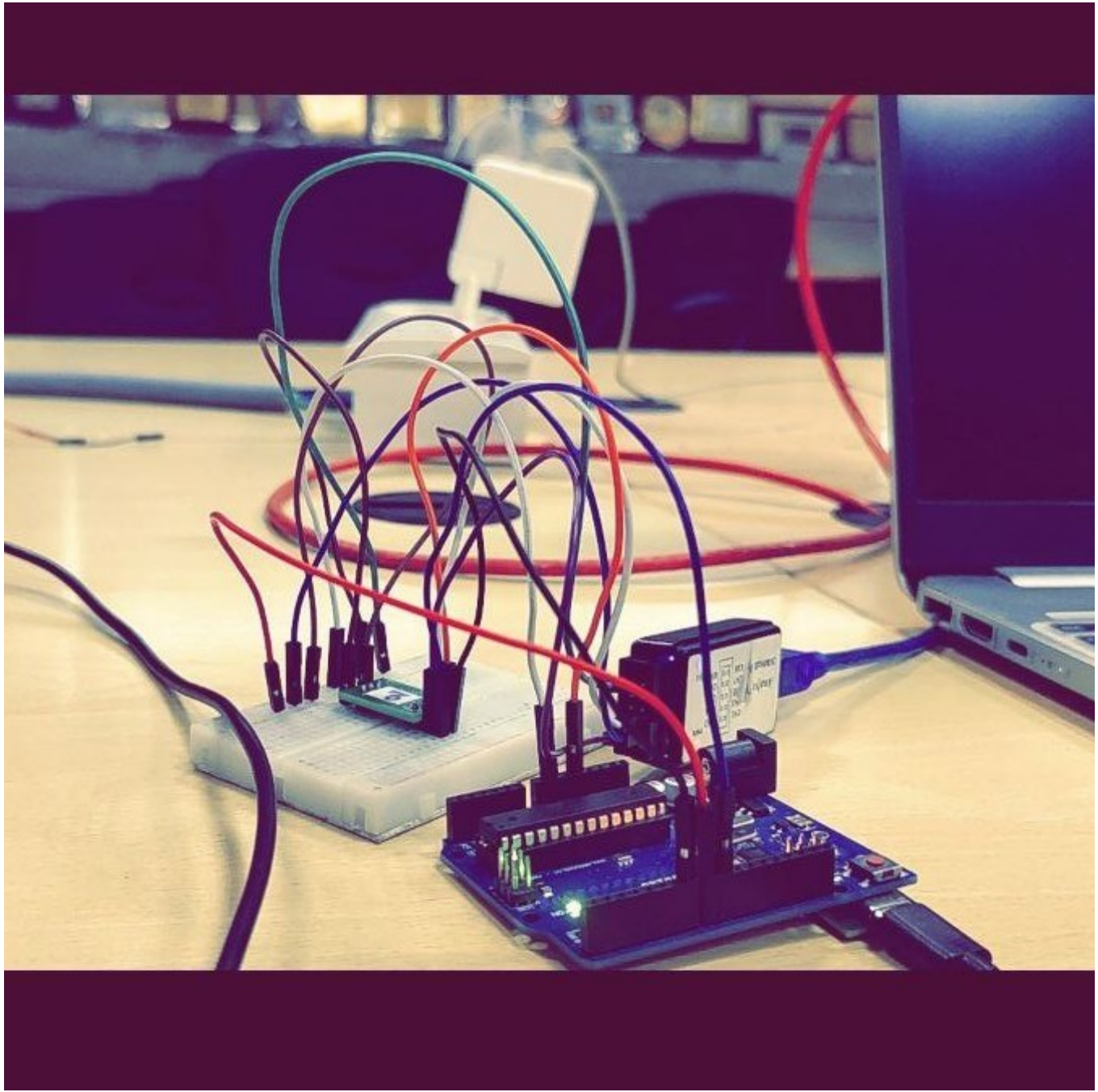


Figure 3:
Caption

Setup



APDU Commands

1. Command: 0x00, 0x84, 0x00, 0x00, 0x08

Explanation:

0x00 - CLA (Class Byte): Standard instruction class.

0x84 - INS (Instruction Byte): Command to generate or get random data.

0x00 - P1 (Parameter Byte 1): Typically used for instruction-specific parameters. In this case, it’s 0x00.

0x00 - P2 (Parameter Byte 2): Similar to P1, also 0x00.

0x08 - Le (Expected Length of Response Data): Requesting 8 bytes of random data.

Purpose: This command asks the card to generate or provide 8 bytes of random data.

APDU Response: 0x84, 0x48, 0x30, 0x65, 0x38, 0x1F, 0xCC, 0xAD, 0x00, 0x90, 0x00

0x84 = initial bit
0x90, 0x00 = SW1, SW2

APDU Commands cont...

2. Command: 0x00, 0x84, 0x00, 0x00, 0x04
   Explanation:
      0x00 - CLA (Class Byte): Standard instruction class.
      0x84 - INS (Instruction Byte): Command to generate or get random data.
      0x00 - P1 (Parameter Byte 1): 0x00.
      0x00 - P2 (Parameter Byte 2): 0x00.
      0x04 - Le (Expected Length of Response Data): Requesting 4 bytes of random data.
   Purpose: This command asks the card to generate or provide 4 bytes of random data.

APDU Response: 0x84, 0xEF, 0x6E, 0xBE, 0xF3, 0x90, 0x00

0x84 = initial bit
0x90, 0x00 = SW1, SW2