SIM driver presentation

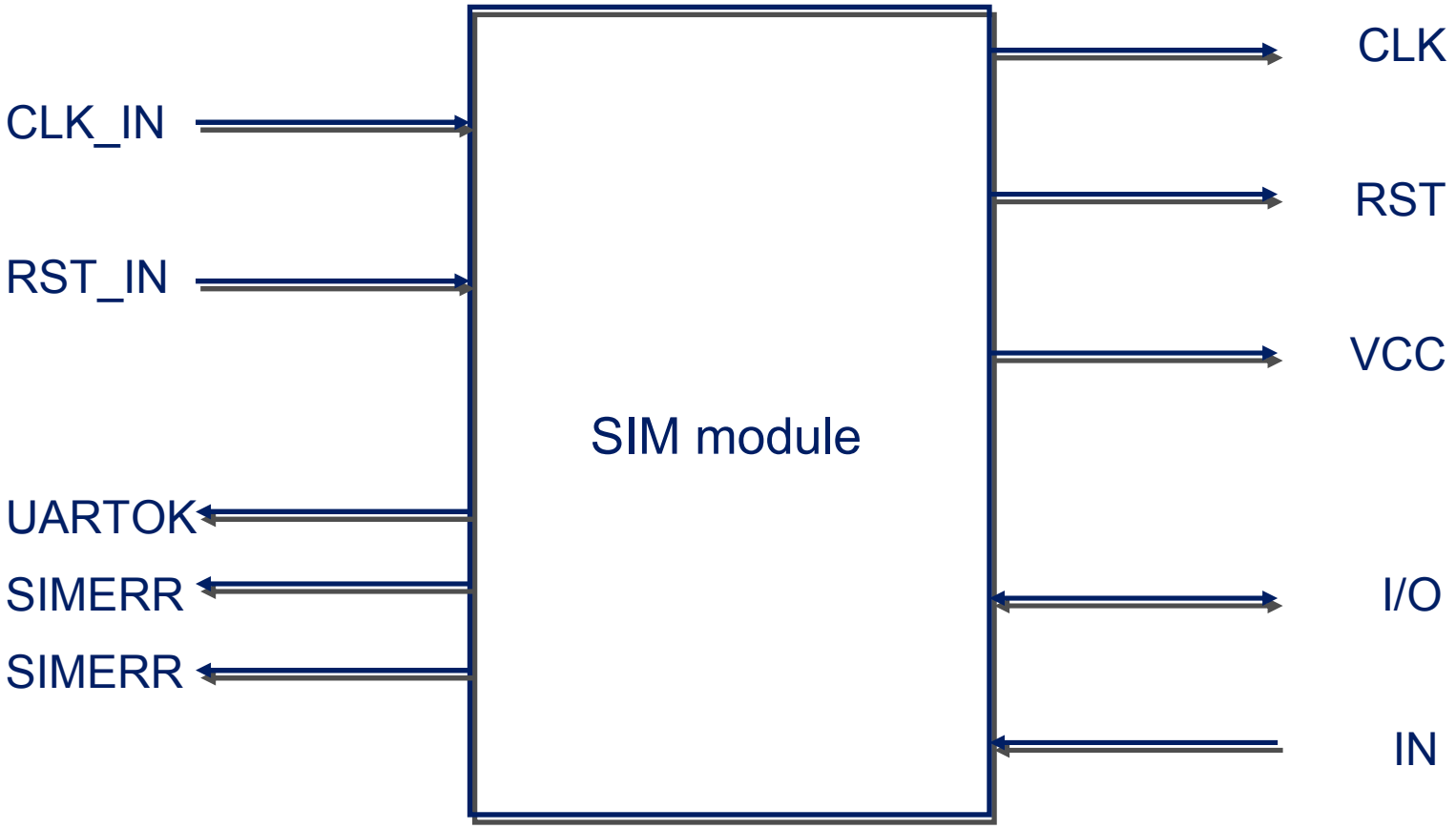
SIM DRIVER PRESENTATION

NEONSEVEN

Purpose of the SIM driver

- Performs SIM activation and deactivation according to ISO-IEC 7816-3, controlling all electrical signals
- Handles the Answer To Reset (ATR)
- Performs the Protocol and Parameter Selection (PPS) procedure – if needed
- Executes APDU commands according to the T=0 Protocol

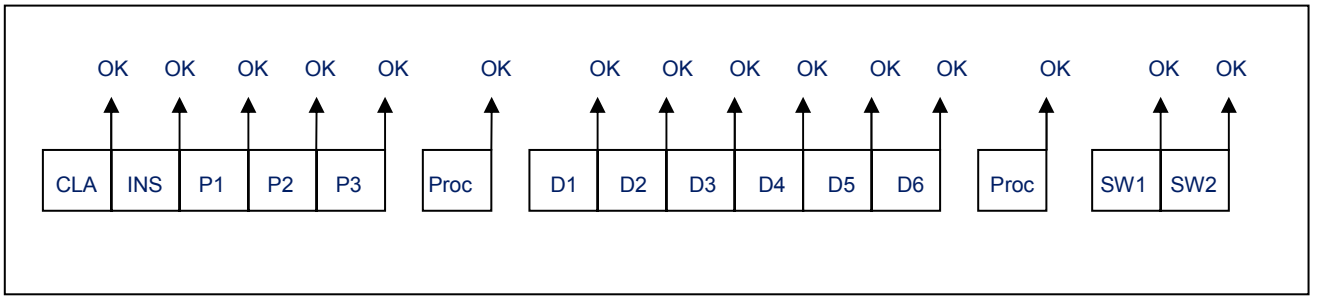
The EGoldRadio SIM interface



NEONSEVEN

SIM Character Mode

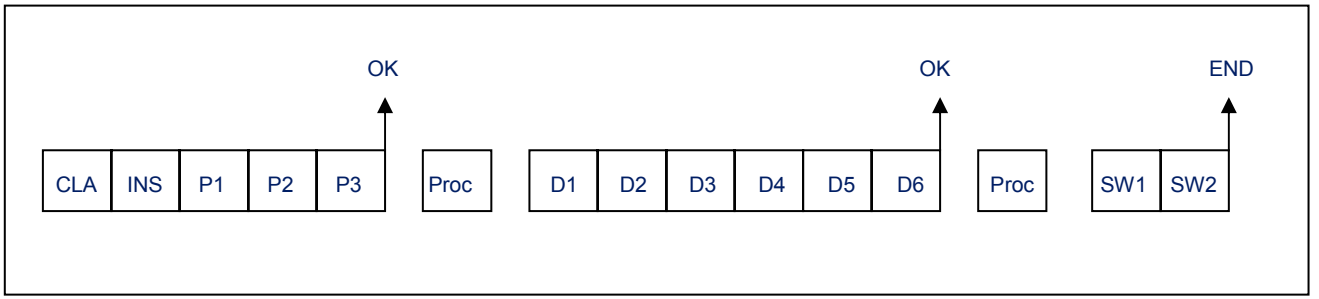
- The SIM UART generates an interrupt for every character (every 1.37ms at normal speed)
- The SIM UART automatically performs only parity retransmission and signalling
- The communication Protocol must be implemented in SW
- Procedure bytes must be handled by SW



NEONSEVEN

SIM T=0 Protocol Mode

- The T=0 Protocol is implemented in a HW block, named HW T=0 Controller
- It automatically handles procedure bytes (acknowledgements and status words)
- It can be easily combined with a PEC channel to minimize SW intervention (for supporting high speed SIM Cards)

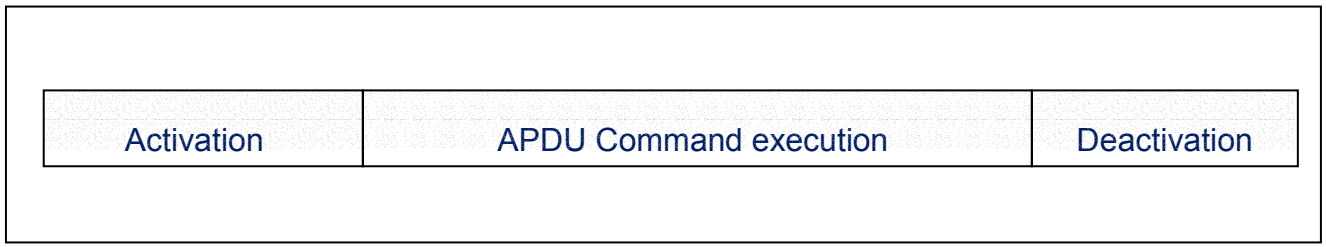


NEONSEVEN

Card session phases

- A SIM Card session is divided into three phases

1. Activation (ATR interpretation and PPS execution)
2. APDU command exchange (CI=slave, SI=master)
3. Deactivation (on SI request or fatal errors)

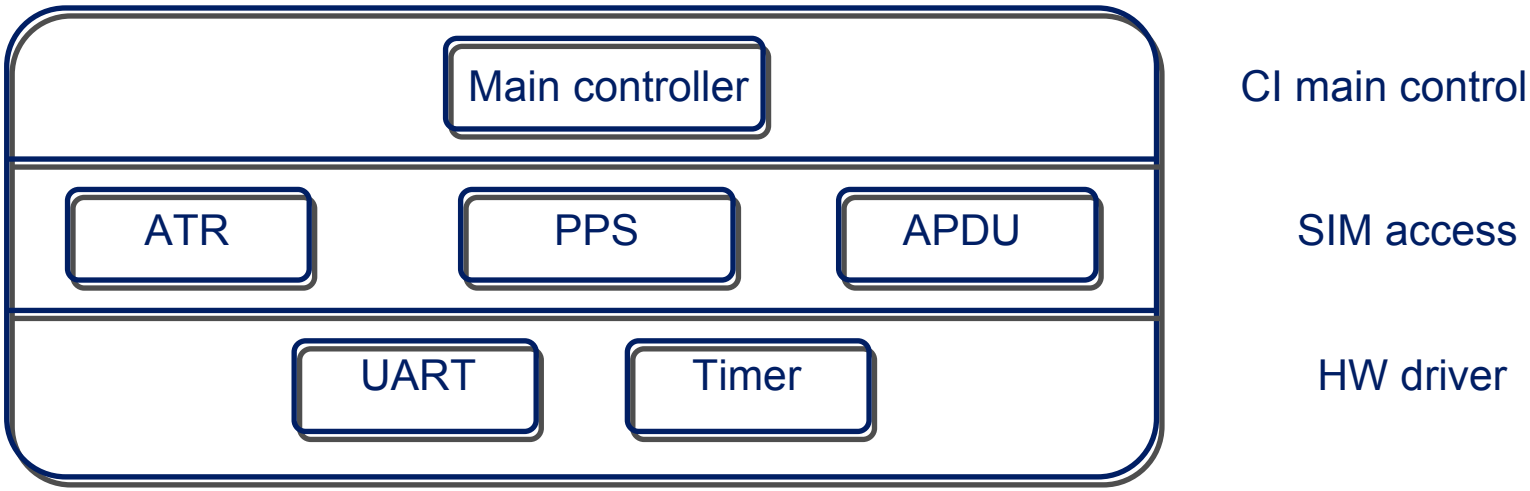


NEONSEVEN

Software architecture (1)

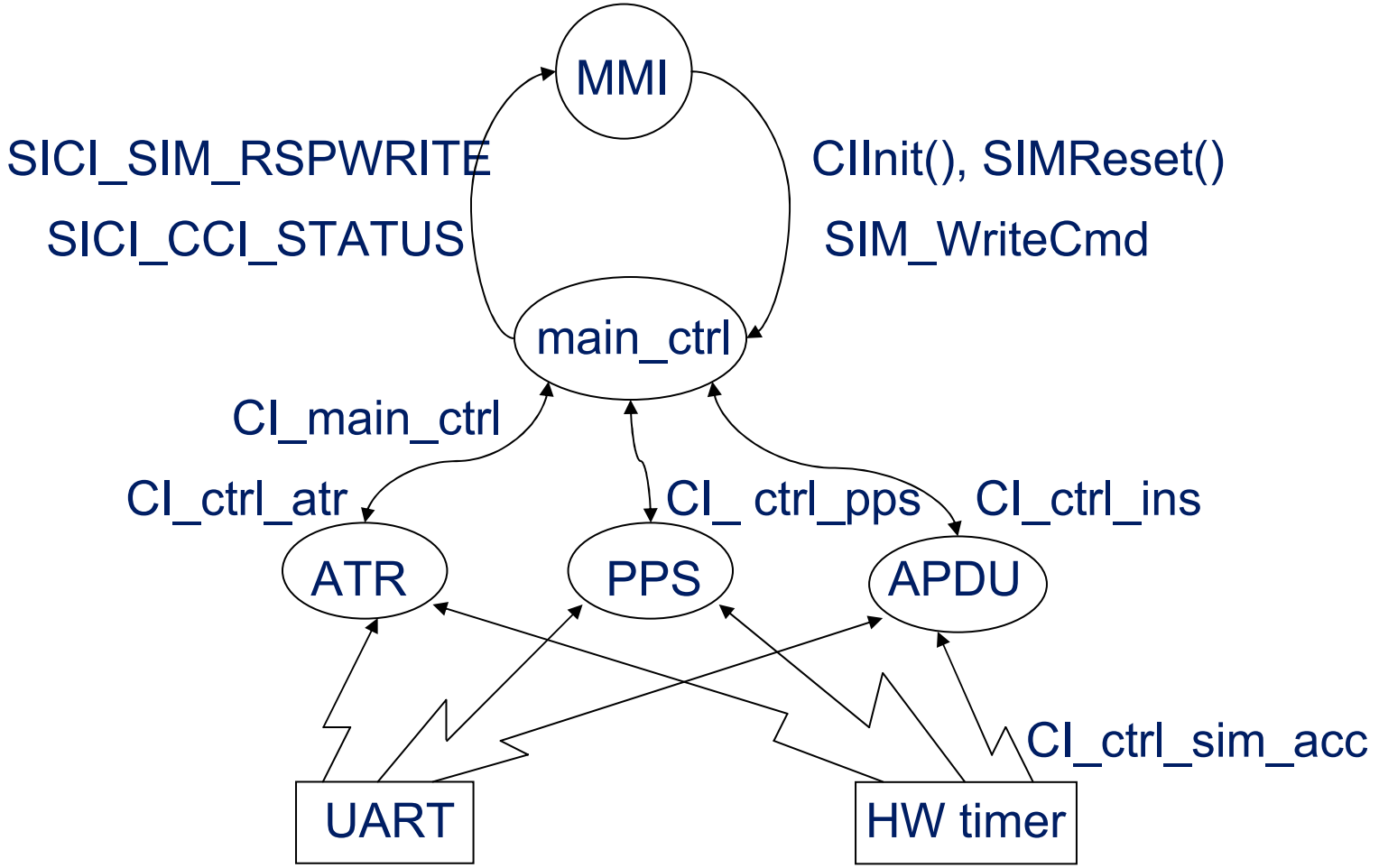
- The SW is divided into three layers

1. Main controller: main state machine
2. SIM access: ATR, PPS and APDU dedicated engines, driven by the main controller
3. HW drivers: SIM UART and HW Timer



NEONSEVEN

Software architecture (2)



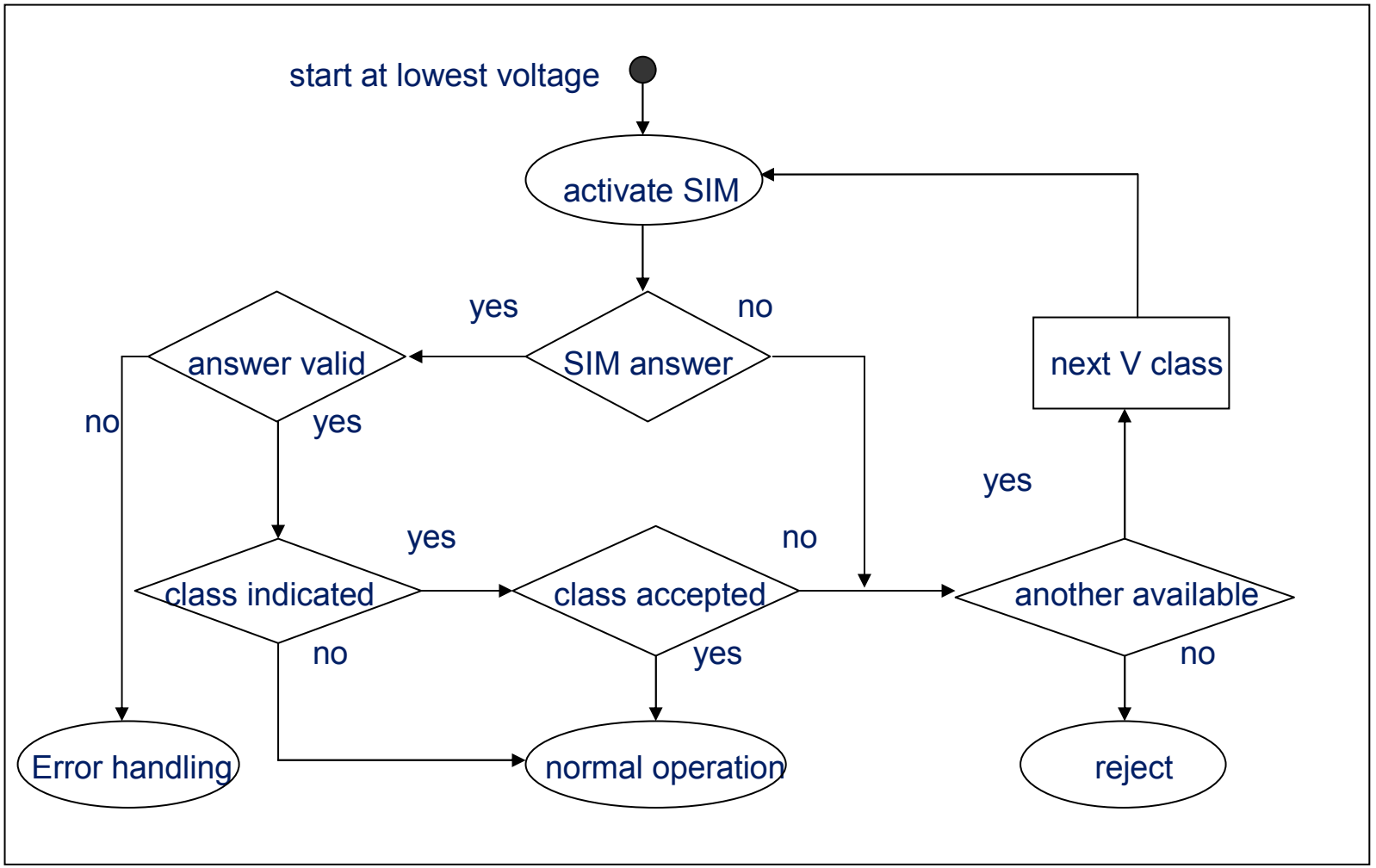
NEONSEVEN

CI main control

- The main controller tasks are:

1. Activate the SIM contacts at power up and receive and interpret the ATR characters.
2. Command the PPS negotiation procedure - if needed.
3. Execute APDU commands towards the SIM – on request from SI.
4. Deactivate the SIM contacts at power down or on request from SI.

Voltage switching



NEONSEVEN

ATR handler

1. Performs electrical activation in the order Vcc, I/O, CLK, RST, operating the SIM card interface in character mode
2. Extracts the clock rate convention factor (FI) and the baud rate adjustment factor (DI)
3. Calculates the guard time from the extra guard time factor N given in TC(1)
4. Calculates the minimum Work Waiting Time from WI in TC(2)
5. Receives and verifies the checksum character
6. Informs CI main control of the activation result

NEONSEVEN

PPS handler

1. Performs the Protocol and Parameter Selection procedure if requested by CI main control
2. If the SIM is suggesting an acceptable F & D pair, a PPS request is issued using these values
3. Only the mandatory values F=512, D=8 are supported
4. Reprograms the Baud Rate Factor register SIMBRF accordingly
5. Notifies CI main control of the procedure result

NEONSEVEN

APDU handler

1. Is responsible for executing APDU commands - one by one - towards the SIM Card
2. Works in T=0 Protocol Mode
3. Combines the HW T=0 controller with a PEC channel, which take care of procedure bytes and data transfer
4. Directly handles only 3 interrupts: at the end of header transmission, data exchange and status response
5. Notifies CI main control of the command result (SW1, SW2)
6. Handles clock stop (mode and level)

UART driver

Provides functions for:

1. Initialising the UART and related interrupts
2. Transmitting and receiving single characters on the serial I/O line
3. Enabling automatic parity error detection
4. Selecting transmission convention (direct or inverse)
5. Selecting the operating voltage (either 1.8V or 3V)
6. Resetting the SIM Card
7. Activating the clock
8. Setting the bit rate

NEONSEVEN

Timer driver

- Provides proper time spacing between electrical signals
- Implements guard timers for unblocking the FSM in case no response is received from the SIM Card
- Offers functions for:

1. Initialising the timer and related interrupt.
2. Starting a timer of variable length meeting the requirements of ISO/IEC 7816-3.
3. Starting a guard timer with fixed length (PPS request character spacing).
4. Stopping a previously started timer.
5. Handling the expiration of a previously started timer.

NEONSEVEN

SI Synchronous interface

- MMI to driver: synchronous (function calls)

1. SIM_WriteCmd: sends a formatted APDU to the SIM Card
2. SIM_SetCardPara: provides voltage and clock stop information to the SIM driver
3. SIM_ResetCard: forces a SIM reactivation (see voltage switching, SAT Refresh)
4. SIM_DeactivateCard: deactivates the SIM Card interface (power off)

NEONSEVEN

SI Asynchronous interface

- Driver to MMI: asynchronous (SDL Signals)

1. SICI_CCI_STATUS: signals a state change (unsuccessful instruction execution, invalid data received, instruction request while busy)
2. SICI_SIM_RSPWRITE: carries the APDU command result SW1, SW2)

NEONSEVEN

Other interfaces

- ATC interface

1. CI_GetSIMStatus: detects whether the SIM Card is operational or not
2. CI_EnterTestMode: sets CI driver in test mode for production

- Power down interface

1. CI_PowerDownAllowed: determine whether CI can accept power down (no ATR/PPS/APDU procedure is in progress)