EMBEDDED SECURITY SYSTEMS, (fake) exam 22.06.2015

Name: .....

Problem 1 Read a specification of commands for a smart card serving as an electronic purse. Reconstruct the logic of the system on the card and analyze its security.

Problem 2 Read the specification of Flyweight from the lecture notes (not presented due to lack of time).

(a) Analyze the role of flags `cnt`, `cnt'`, `alarm` and `alarm'`. Analyze the protocol behavior in case when their values are fixed to 1?

(b) Consider an adversary that may selectively jam the messages sent between the reader and the card. Show that the adversary cannot desynchronize the reader and the card.

Problem 3 In the UMTS AKA protocol the SQN parameter is checked to be within a certain interval.

What is the attack that this mechanism is responding to? Propose a mechanism for determining the width of this interval.

Problem 4 Can a TPM device be used as a secure device for creating electronic signatures? (It is less likely to loose a laptop with TPM than a chip card. Finally, the access protection for a laptop can be far more sophisticated than the PIN control form the smart card.)