Embedded Security Systems
Laboratory Tasks 4

Deadline: 11.05.2017

Task 1 (20%)

Create a java card applet that generates an elliptic curve key pair. You can use the class `KeyPair` to store and generate new keys from empty `ECPublicKey` and `ECPrivateKey` keys created using the `KeyBuilder` class.

Task 2 (30%)

Create a java card applet that can be used to store data. Each data group should be 128 bytes long. The applet should support about 6 data groups. The applet should support instructions `INS=0x10` for writing, `INS=0x20` for reading and `INS=0x30` for deleting (i.e. zeroing), where parameter `P1` should indicate the data group.

Task 3 (50%)

Use the `javax.smartcardio` class from Java SE to create a terminal application (see example `https://docs.oracle.com/javase/7/docs/jre/api/security/smartcardio/spec/`). Use this application to demonstrate task 1 and 2. In case of task 2, try to create a GUI that allows to change the data stored in a given data group.