Embedded Security Systems
Laboratory Tasks 6

Deadline: 22.06.2017

Mini Project (100%)

Create a java card applet that can be used to store data in a similar way as in task 2 - lab tasks 4. However, only a known reader should be able to read and write data. Thus, your application should implement a way to authenticate the reader and secure communication.

In order to do so, you can use the code from task 1 - lab tasks 5. However, instead of using a random public key of the reader, you should implement a special instruction e.g. INS=0x40, that can be executed only once and stores the public key of the reader (this is called static Diffie-Hellman protocol). Once you generate the shared secret key with the reader, both sides should use Authenticated Encryption (see `https://en.wikipedia.org/wiki/Authenticated_encryption`) to communicate.

HINT: Authenticated Encryption can be implemented using the Encrypt-then-MAC paradigm (you can use the `Cipher` class for `AES` encryption scheme and the `Signature` class for computing message authentication codes `MAC`).