Exercise 4

OO: Applet Design, Java Card RMI, Optimizations

In this exercise, you will design an applet from start to finish.

The applet shall function as a password “vault”. The applet stores passwords belonging to different web sites. The host will provide a URL (e.g. as byte array), which the applet can associate with passwords. The applet should offer functionality to create, retrieve, and delete passwords. Access to passwords should be protected with a PIN (use the OwnerPIN API provided by Java Card), which the user should be able to change, or unlock with a special unlock key (PUK) if blocked. Initial PIN and PUK values should be set during applet installation using the install parameters.

You are to define the command and response APDUs, and implement the applet accordingly. You are free to choose any strategy for associating URLs with passwords, keeping in mind that performance is most often crucial on a resource-constrained device. Try to make use of the optimization concepts discussed and demonstrated during the lecture.

Note: Although this is potentially insecure, you do not need to protect passwords stored in EEPROM with encryption.

Furthermore, you are to define a remote interface, which your applet shall implement. This remote interface should offer all the functionality available through the “normal” APDU interface.

You do not need to implement an off-card client (yet…).