HSM project

Documentation (Desktop application)

Ismail Lotfi 4.5.2017

Introduction:

We have modified the original source code of the JPass application to respect the HSM mechanism. There was only one file edited “MessageDialog” and a new package “applets” have been added to communicate with the card.

Applet package:

It contains two classes “MyApdu” and “CardMngr” . The first one is responsible for preparing the APD commands, the second one is for sending and receiving data from the JavaCard. All the functions are self documented in the source code.

“MessageDialog” class:

The function “showPasswordDialog” was edited, where we replaced the password with a PIN text field and sent this PIN to the javaCard. Depending on the result, the function will send another command to get the encryption key or ask the user again to set the PIN. If the user fail 5 times to set the PIN, he will be asked to set the PUK (the limits number can be edited depending on the vendor’s decision) to reset a New value to the PIN.