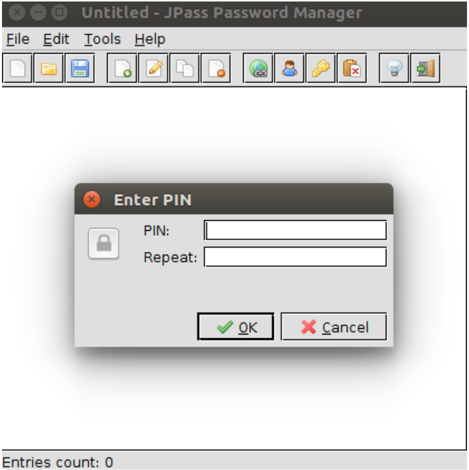
HSM project

Deniz Agaoglu, Jerguš Lysý, Ismail Lotfi

May 4, 2017

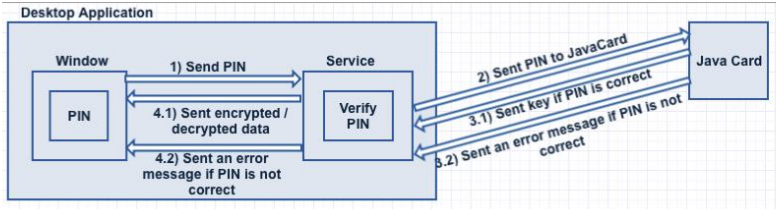
Design — previous design



Design

- Based on JPass project.
- The user set a 4 digit PIN instead of a password.
- JavaCard verify if the PIN is correct, if yes the encryption key is sent to PasswordSafe Application to perform the Encryption / Decryption, else the user can set at maximum 5 Wrong PIN.
- If the user exceed the limits, he is asked for a secret that he has already saved in a safe location. If the user fail to set this secret the JavaCard is blocked.

Design — new design


Desktop Application
Window
PIN
1) Send PIN
Service
Verify PIN
4.1) Sent encrypted / decrypted data
4.2) Sent an error message if PIN is not correct
2) Sent PIN to JavaCard
3.1) Sent key if PIN is correct
3.2) Sent an error message if PIN is not correct
Java Card

- Communication between the Desktop application and the JavaCard is using secure Channel (GP API).
- AES key is used to encrypt data.
- Automata based programing.