SI5/M2II - IoT Security Lab
October 23rd, 2023
Yves Roudier - UCA / Polytech Nice Sophia
Smart Card Project Description

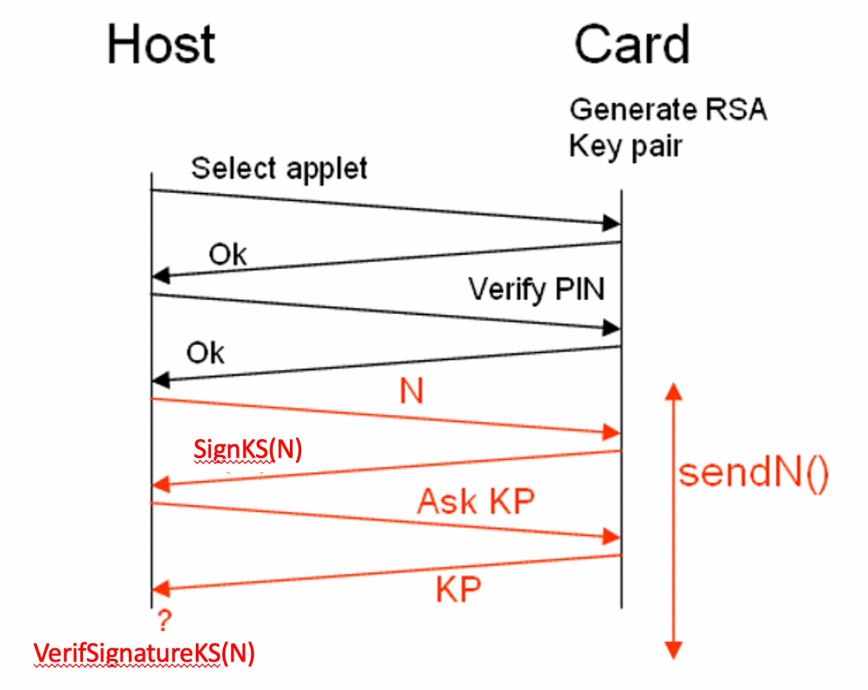
In this project, you will have to develop a terminal + a smart card supported application, which should make it possible for you to generate an RSA private and public key pair within the smart card. The terminal application will send some data to the smartcard and will retrieve its encrypted version and the public key for verifying the encryption.

1) The smart card applet

You first have to implement a JavaCard applet that should support the following functionalities:

- The card should be protected with a PIN code that will be provided by the end-user
- The card will have to generate an RSA 512-bit key pair
- The card will be able to sign a data transmitted by the terminal-side application on demand, thus playing the role of a minimalistic TEE
- The card will transmit its public key to the terminal side of the application on demand

You will have to implement the sendN() method which should behave according to the following protocol:



The transmission of some data (typically N and its signature) may involve multiple APDUs and their reassembly if too large to be sent over a single one.

2) The terminal side application

You will have to implement a standalone application running on your computer, that is, on the terminal talking to the smartcard.

You can write this application in Java, using one of the approaches outlined in the lab document, or in other languages like Python for instance.

This application will need to interact with the end-user to request a PIN code and should make it possible to load the data to be encrypted from a file and to store the result of the encryption to another file.

The application should also make sure that the data are correctly signed based on the public key received from the smart card. The terminal side here simulates the behavior of a third party application interacting with the terminal.

3) Report and Results

You have to provide:

- a small report describing the architecture you adopted and how you tested your development. It is suggested to test your applet methods using interactive APDU messages
- The applet should be loaded on your Javacard
- You will have to provide your terminal-side application and its documentation. Make sure that it can be started from the command-line and don't forget to provide any dependencies that may be required.