HSM Project
JavaCard Applet

Documentation

Jerguš Lysý **1.5. 2017**

Table of Contents

1 Introduction

For the purposes of the HSM project the JavaCard applet has to be implemented as the working key provisioner for the application. This document shall specify this part of the project in more detail as well as the implemented applet.

1.1 Design

The aim of the applet is to provide a cryptographic key that is used by the application. The key transmitting is made in a rather secure way, which consists of the following main features:

- Secure channel opened on JavaCard using three cyrptographic keys.
- Key protected by a PIN (required from the application) and PUK (set during applet installation).
- Protected from running any applet functions by using automata-based programming approach.

All of these three concepts are introduced in the applet and are discussed in the following sections. The implementation of these features is described in the next chapter. The last two chapters present the usage of secure domain of Global Platform and scripts needed for an applet installation and testing.

1.2 Securing applet

For the security of the overall project the secure channel must be initialized between the application and the applet. At least these aspects have to be reached to preserve such a security:

- Mutual authentication of the JavaCard a the application.
- Integrity and confi of APDUs

For this purpose the Security Domain on JavaCard. This domain has been installed into the card with provided all of the mandatory keys. The application and