

Chipsets Programming

Disclaimer

This follows the lessons from Mr. HADIOUCHE Azouaou given in course, major additions, changes or rearrangements can be applied on the course for the sake of clarity, better explanations or just subjective opinions, written by HOCINE.

USE THIS AT YOUR OWN RISK.

Chapter 1

Introduction

This course will be talking about programming cards, both from the card and software that comes with it, and how to implement card instructions. Cards are used in multiple domains to simplify authentication or access to services such as identification and bank services.

1.1. Types & Architecture

Cards can be divided into two types:

- Contact Cards: that has its chipset exposed directly outside and the reader would use the pins to communicate with the card, which is categorized into
 - Cards with logic gates printed directly on the card.
 - Cards with a micro-controller inside that enables reprogrammability.
- Contactless Cards: an advanced technology where the card has its chipset inside and the reader uses radio frequencies to communicate the data of the card, this technology uses micro-controller directly since it was available at the time of the development of contactless communication.

1.1.1. Card Micro-controller

The micro-controller is the unit englobing the micro-processor and all the parts needed to run it, here are the components of the micro-controller

- **Control Unit:** the micro-processor along with a unit to control the flow of data between the parts of the micro-controller, the processor is usually 16 or 32 bits.
- **PROM/EEPROM:** (Programmable Read Only Memory/Electrically Eraseable Programmable Read Only Memory) which store the program that would be run by the card to interface with the reader, the amount of storage varies from 1KB to 128KB or 256KB for Java Card.
- **RAM:** (Random Access Memory) which stores the variables and dynamic data for usage and would be erased after the communication between the card and reader is done.

- **I/O Interface:** an interface to be able to communicate with I/O devices.
- **Crypto Processor:** a CPU made specially for cryptographic operations and contains multiple physical security measures to keep the user safe.

The card uses a simplified UART to interface with the reader, and by default the card contains an OS that can run a smaller JVM (Java Virtual Machine) that allows to run a specific framework for Java called Java Card on the card's micro-controller.

Java Card has less features than Java given that it runs on a hardware that is a lot weaker than the usual computer. We will go through some of these missing features.

- Missing primitive data types:

Type	Size (bits)	JavaCard Support
boolean	1	✓
byte	8	✓
short	16	✓
int	32	✓
long	64	✗
double	64	✗
char	8	✗
float	32	✗

- Missing compiler/interpreter features:
 - serialization, threads and parallelism.
 - dynamic loading or hot-reloading.
 - cloning and multi-dimensional arrays.

We will use all the features included in Java including the OOP paradigm.