Государственное образовательное учреждение
высшего профессионального образования
Московский государственный индустриальный университет

Кафедра «Информационные системы и технологии»

ДИПЛОМНАЯ РАБОТА

по специальности «Математическое обеспечение и администрирование информационных систем»

Сергеева Дмитрия Александровича

на тему

«Реализация Java – апплета с открытым кодом в Aladdin eToken для аутентификации пользователей сети ГОУ МГИУ»

Научный руководитель: **Бургонский Д.С., доцент**

Москва 2010

Что такое eToken?

eToken:

- Устройство, снабженное микропроцессором, памятью, устройствами приема и передачи информации.
- eToken может быть снабжен микросхемами памяти трех типов:
  - Постоянной неперезаписываемой (ROM)
  - Постоянной перезаписываемой (EEPROM)
  - Оперативной (RAM)

Цель работы

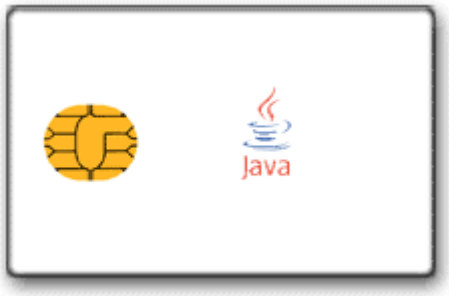
Целью данной работы является:

- Разработка Java–апплета для Aladdin eToken PRO (Java) .
- Разработка хост–приложения соответствующего Java–апплету.

Технология Java Card

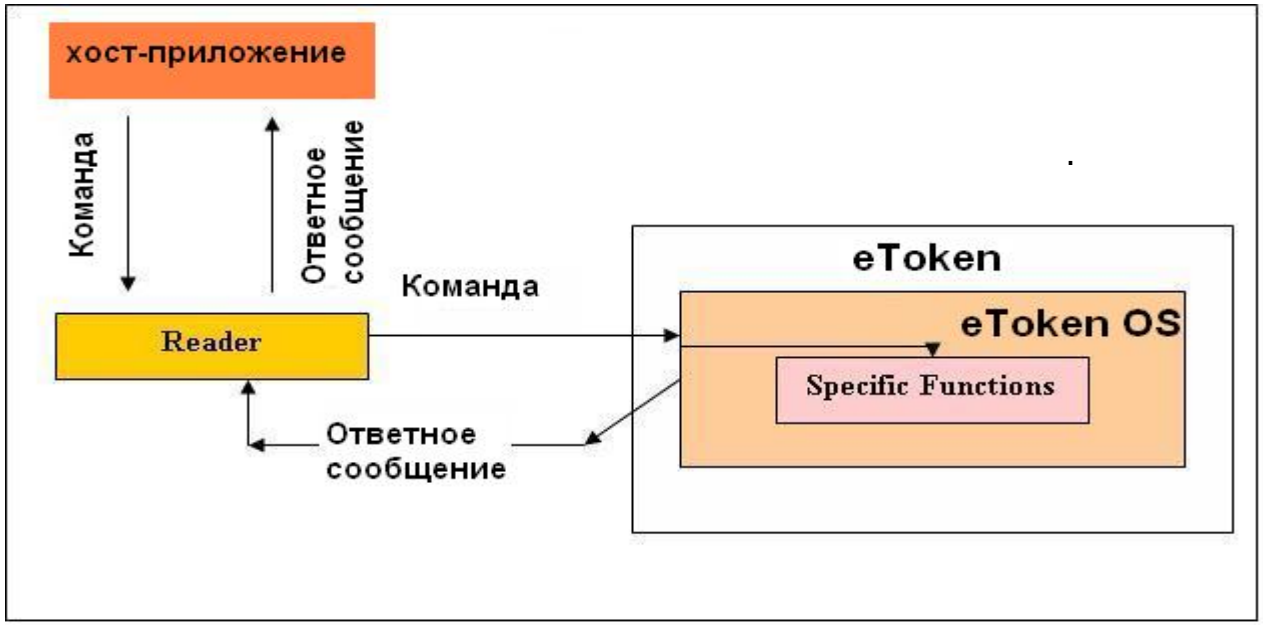
Технология Java Card позволяет исполнять программы, написанные на языке программирования Java, на eToken PRO (Java) и других вычислительных устройствах с ограниченными ресурсами.

- Приложения, написанные для платформы Java Card называются, апплетами. Название было выбрано из схожести модели выполнения со стандартными апплетами, исполняемыми в виртуальной машине Java (JVM) веб-браузера.



Принцип взаимодействия с хост-приложением

Общение eToken происходит по средствам пакетов данных, которые называются APDU (Application Protocol Data Units). Пакеты APDU содержат либо команду, либо ответное сообщение. Технология eToken моделирует интерфейс "ведущий-ведомый" (master-slave), в котором самому eToken отводится пассивная роль. Другими словами, eToken всегда ждет от хост-приложения команду APDU. Затем он выполняет указанное действие и посылает хост–приложению ответный пакет, подтверждающий выполнение команды. Между eToken и хост-приложением происходит непрерывный обмен пакетами APDU, содержащими команды и ответы на них.



Структура пакета APDU

Обязательный заголовок				Условное тело команды		
CLA	INS	P1	P2	Lc	Поле данных	Le

В заголовке кодируется выбранная команда. Она состоит из четырех полей: класс (CLA), инструкция (INS), параметр 1 и параметр 2 (P1 и P2). Каждое поле имеет размер 1 байт.

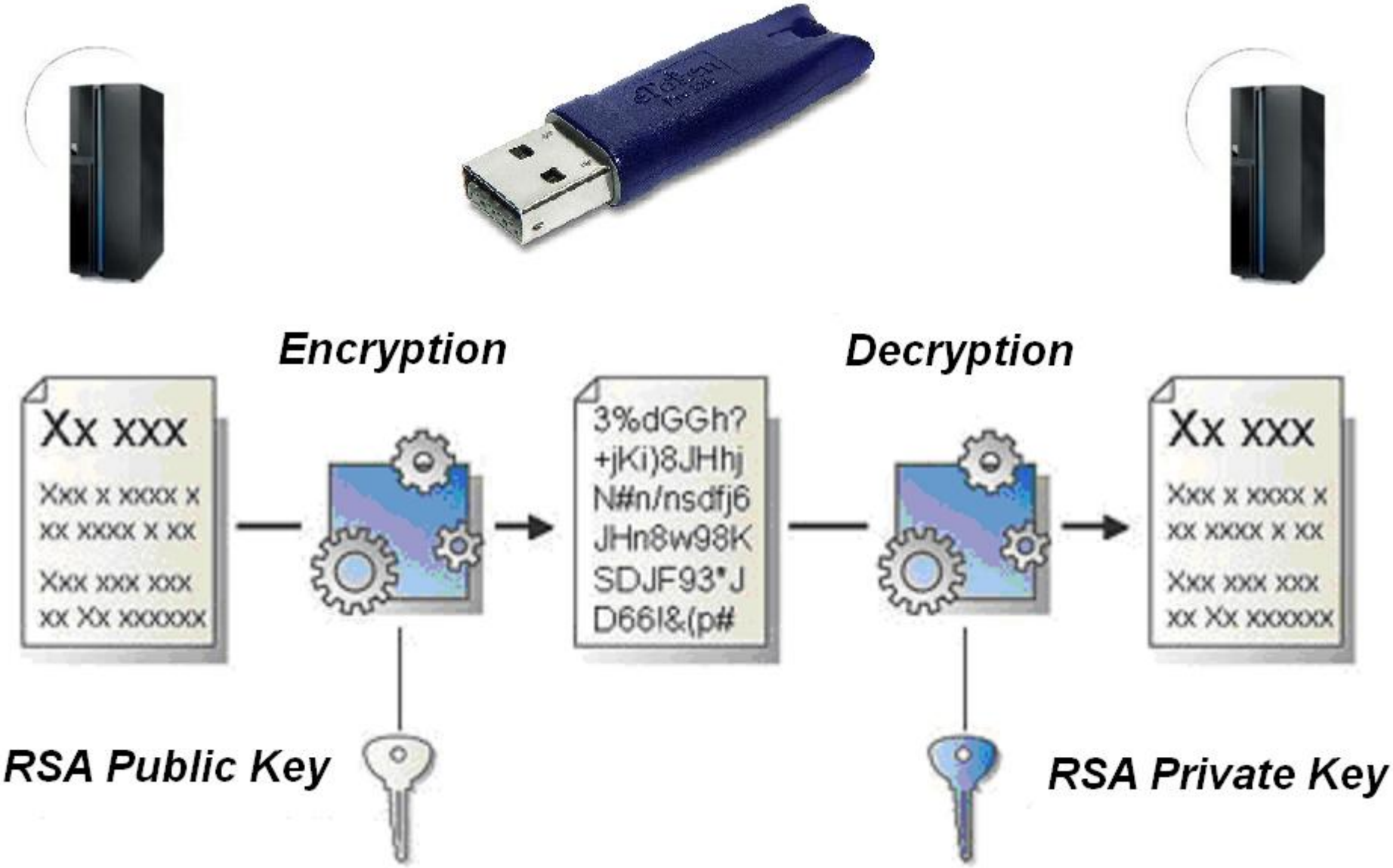
- CLA: байт класса. Во многих eToken данный байт используется для идентификации приложения.
- INS: байт инструкции. В этом байте содержится код инструкции.
- P1-P2: байты параметров. Данные байты содержат дополнительную характеристику команды APDU.
- В поле Lc размещается количество байтов в поле данных команды APDU.
- В поле Le заносится максимальное количество байтов, которое может находиться в поле данных ответного APDU.

Условное тело ответа	Обязательная концевая часть	
Поле данных	SW1	SW2

Байты состояния SW1 и SW2 обозначают статус обработки eToken команды APDU.

Принцип работы

Схема аутентификации



1. Реализованный Java-апплет поддерживает следующее:
    - Использование PIN кода для защиты данных апплета.
    - RSA секретный ключ.
    - Аутентификация.
2. Реализованное хост–приложение осуществляющее, процесс аутентификации Java–апплета на eToken PRO (Java), поддерживает следующее:
    - Верификацию PIN кода.
    - Генерацию RSA ключа.
    - RSA открытый ключ.
    - Аутентификацию Java–апплета.