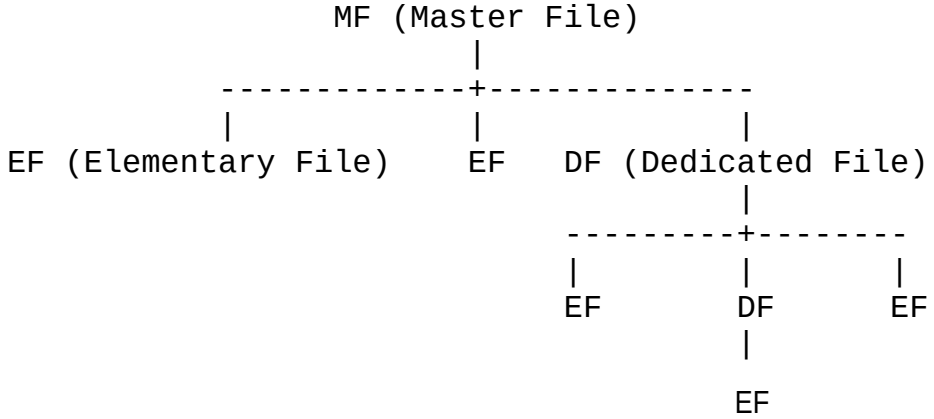
Smart Cards.

Павленко А. А. , гр. 917.

История смарт-карт начинается с 1976 года, когда фирма CP8 Transac анонсировала первую в мире пластиковую карточку со встроенной микросхемой. В 1978 году эта фирма запатентовала архитектуру SPOM (Self Programming One-chip Memory), которая по сегодняшний день является стандартом внутренней организации смарт-карт.

Согласно SPOM в смарт-карте предусматривается наличие постоянной памяти (ROM) на кристалле, оперативной памяти (RAM) и постоянной перезаписываемой памяти (EEPROM). Обычно смарт-карта представляет собой маленькую пластиковую карту со встроенным микропроцессором и памятью. Но, несмотря на маленькие размеры и простую структуру, смарт-карты получили широкое распространение и применяются во многих отраслях. Они могут использоваться как : телефонные карты, карты идентификации личности, дверные ключи и т.д. ...

Информация на смарт-карте хранится виде файлов и может считываться различными программами, в зависимости от операционной системы карты. Структура файловой системы, в которой хранятся файлы, схожа со структурой директорий в Linux.



MF (Master File) – корневая директория.

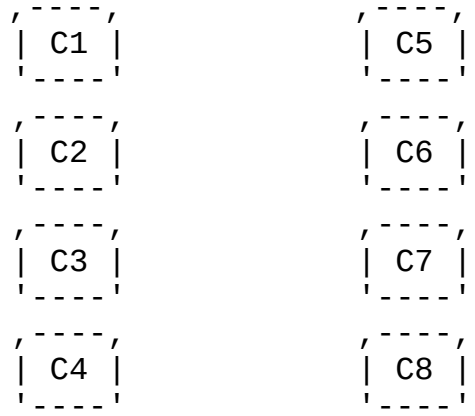
DF (Dedicated File) – обычные директории.

EF (Elementary File) – файлы с данными.

Так как в смарт-картах есть встроенный микропроцессор, необходима энергия и некоторые устройства, что бы “общаться” с картой. Некоторые карты имеют

контакты. Такой тип смарт-карт называется “*Contact* Smart Cards”. Эти контакты используются для снабжения электроэнергией и для осуществления связи с различными устройствами.

Схема контактов, в соответствии со стандартом ISO7816 :



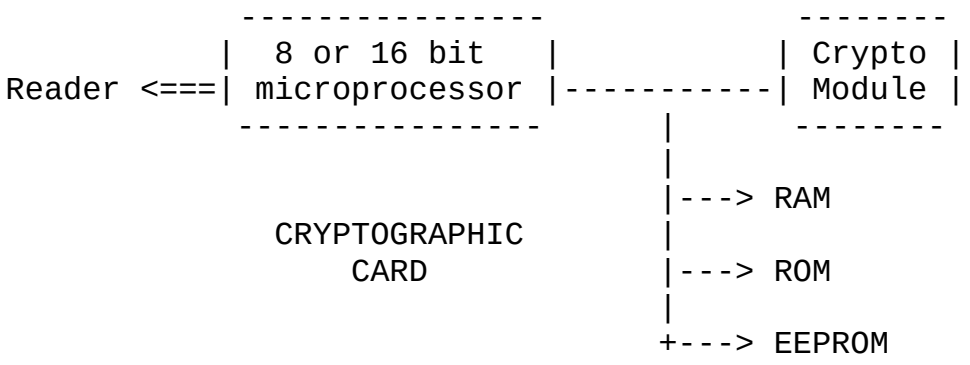
C1 : Vcc = 5V C5 : Gnd
C2 : Reset C6 : Vpp
C3 : Clock C7 : I/O
C4 : RFU C8 : RFU

Существуют так же и бесконтактные смарт-карты. В таких картах взаимодействие с различными устройствами осуществляется с помощью радио волн. В них встроена маленькая катушка индуктивности. Эта катушка используется как индуктор для обеспечения энергией и для связи с устройством. Когда карта вставляется в считывающее устройство в катушке индуктивности, под воздействием переменного магнитного поля, индуцируется ток и она используется как источник энергии.

Наиболее распространенные и наименее дорогие смарт-карты – карты с памятью. Этот вид карт содержит EEPROM(Electrically Erasable Programmable Read-Only Memory) и является энергонезависимым, благодаря чему, когда вы удаляете карту из считывающего устройства, то есть отключаете электропитание, карта сохраняет данные. EEPROM – это обычное устройство ля хранения информации, которое имеет файловую систему и управляется посредством микроконтроллера. Этот микроконтроллер отвечает за доступ к файлам с данными и обеспечение связи с внешними устройствами. Данные могут быть заблокированы с помощью PIN (Personal Identification Number) - персонального пароля. PIN обычно от 3 до 8 символов которые записаны в специальном файле на карте.

Карты со встроенным микропроцессором скорее являются компьютерами. В них есть RAM, ROM и EEPROM со встроенным микропроцессором. Так же в картах этого типа есть операционная система, с помощью которой можно управлять файловой системой EEPROM и запускать необходимые функции в RAM. Операционная система смарт-карты представляет собой набор процедур, управляющих работой процессора. В настоящее время существует много различных операционных систем для смарт-карт. Выбор определенной операционной системы зависит от приложения, в котором она будет работать. Операционные системы, как правило, служат для обеспечения безопасности хранящихся данных и для выполнения операций с файлами. Операционная система, как правило, разрабатывается изготовителем смарт-карты и хранится в ROM памяти. Некоторые смарт-карты позволяют расширение стандартных возможностей смарт-карты путем загрузки дополнительных программных модулей в EEPROM память.

Процессор, находящийся в смарт-карте, отвечает за разграничение доступа к хранимой в памяти информации и за выполнение процедур обработки данных. Многие смарт-карты снабжаются специальным процессором для выполнения операций с большими числами для генерации простых чисел при использовании асимметричных криптографических алгоритмов.



Как видно из диаграммы передача данных осуществляется через процессор, нет прямой связи между памятью и контактами. За безопасность данных, хранящихся в памяти, отвечает операционная система. Данные шифруются с помощью специального криптографического модуля.

В постоянной памяти (ROM) хранится исполняемый код внутреннего процессора, оперативная память (RAM) используется в качестве рабочей, и, наконец, к перезаписываемой памяти (EEPROM) возможен доступ извне для чтения/записи произвольной информации.

Международная организация по стандартизации ISO приняла ряд стандартов на смарт-карты, объединенных в общую группу ISO7816. На сегодняшний день существует 6 стандартов из этой группы :

- ISO7816-1 Физические характеристики;
- ISO7816-2 Размеры и расположение контактов;
- ISO7816-3 Электрические сигналы и протоколы передачи данных;
- ISO7816-4 Высокоуровневые команды для обмена;
- ISO7816-5 Система регистрации приложений в смарт-картах;
- ISO7816-6 Высокоуровневые элементы данных.

Основным требованием к смарт-карте при ее проектировании является высокая степень защиты данных, хранящихся на ней. Под надежностью понимается как физическая, так и логическая защищенность данных. Логическая защищенность реализуется следующими путями :

- аутентификация карты;
- аутентификация терминала (устройства, работающего с картой);

- идентификация пользователя;
- использование механизмов разграничения доступа к данным;
- криптографическая обработка данных;
- использование механизмов электронной цифровой подписи;
- полный контроль микропроцессором всех операций чтения/записи с EEPROM.

Смарт-карта должна обеспечивать полную защищенность данных при изъятии микросхемы из кристалла и попытках считать информацию с кристалла электронными щупами. Это достигается благодаря специальному дизайну кристалла, а, так же, благодаря тому, что все компоненты архитектуры смарт-карты находятся в одном кристалле и имеют минимальные размеры.

Физическая защищенность подразумевает невозможность получить доступ к данным путем изъятия микросхемы из карты и непосредственной работы с ней, и невозможность стирания информации ультрафиолетовым и рентгеновским излучением.

Такая степень защищенности и удобства в использовании делает смарт-карты весьма перспективными во многих применениях.

Список литературы:

- **Обмен данными со смарт-картой**

  http://kbts.mbit.ru/sat/satxpress/SmartCard/ISO7816.htm

- **Smart Card HOWTO**

http://www.350mb.ru/traffic/docs/linux.howto/Smart-Card-HOWTO/index.html

- **Smart Cards**

  http://users.freenet.am/~acidnet5/smartcards.htm

- **Смарт-карты и их применение в электронной коммерции**

  http://kunegin.narod.ru/ref3/sc5/