Смарт-карты

Смарт – карта была изобретена французом Роланом Морено в середине 70-х, но только в конце 1980-х технологические достижения сделали ее достаточно удобной и недорогой для практического использования. В мире наблюдается все более активный переход от магнитных карт к смарт - картам. Европа, где только в 1993 году было выпущено уже более 350 миллионов смарт - карт и карт памяти, занимает ведущее место на этом пути. Большинство экспертов убеждены, что через 10 лет или раньше карточки с магнитной полосой станут частью истории. Последние сообщения VISA подтверждают это.

Внешне смарт - карты похожи на карты памяти, однако микросхема смарт - карты содержит "логику", что и делает эти карты интеллектуальными, по-английски - "smart". Микросхемы смарт - карты представляют собой полные микроконтроллеры (микрокомпьютеры) и содержат следующие компоненты:

* **CPU**(центральный процессор) - Устройство для обработки инструкций карты
* **RAM** (ОЗУ) - Память для временного хранения данных, например, результатов вычислений, произведенных процессором
* **ROM** (ПЗУ) - Память для постоянного хранения инструкций карты, исполняемых процессором, а также других данных, которые не изменяются. Информация в ПЗУ записывается в процессе производства карты.
* **EPROM** (ППЗУ) - Память, которая может быть прочитана много раз, но записана только однократно. В ППЗУ организация, выпускающая карту в обращение, записывает данные о ее владельце
* **EEPROM** (ЭСППЗУ) - Память, которая может быть перезаписана и считана многократно. В этой памяти хранятся изменяемые данные владельца карты. ППЗУ и ЭСППЗУ не теряют данные при отключении питания
* **I/O** (Ввод/вывод) - Система для обмена данными с внешним миром
* **Operating system** (Операционная система или программное обеспечение карты) - Инструкции для процессора, хранимые на карте
* **Security features** (Система безопасности) - Встроенная система безопасности для защиты данных с возможностью их шифрования

Смарт - карта в действительности представляет собой небольшой компьютер, способный выполнять расчеты подобно персональному компьютеру. Наиболее мощные современные смарт - карты имеют мощность сопоставимую с мощностью персональных компьютеров начала восьмидесятых. Операционная система, хранящаяся в ПЗУ смарт - карты, принципиально ничем не отличается от операционной системы PC. ЭСППЗУ используется для хранения данных пользователя, которые могут считываться, записываться и модифицироваться, также как данные на жестком диске персонального компьютера. Смарт - карты имеют различную емкость, однако типичная современная смарт - карта имеет ОЗУ 128 байт, ПЗУ 2-6 КВ и ЭСППЗУ 1-2 КВ. Некоторые смарт - карты также содержат магнитную полоску, что обеспечивает их совместимость с системами на базе магнитных карт. Смарт - карты дороже карт памяти, и также как в случае карт памяти их стоимость определяется стоимостью микросхемы, которая прямо зависит от размера имеющейся памяти. Смарт - карты обычно используются в приложениях, требующих высокой степени защиты информации, например, в финансовой практике.

Применение в финансовой сфере.

**Финансовые карты** используются для выполнения платежей. Финансовые карты, конечно, имеют самую большую потенциальную сферу использования для смарт-карт, и многие задачи управления доступом и хранения информации перекрываются с финансовыми задачами. Легко видеть, какие открываются перспективы в распространении смарт-карт, если учесть, что 2 миллиарда магнитных карт уже находятся в обращении, а, кроме того, Россия и другие страны СНГ, страны Восточной Европы и Китай готовы войти в мировой рынок. Изначально магнитные кредитные карточки были разработаны более чем 30 лет назад для удобства путешествующих бизнесменов, которых в то время было мало. *Они работали хорошо в первоначальной прикладной задачах (и продолжают работать: я сам использую эти карточки почти каждый день), но в девяностые годы, карточки и прикладные системы разрабатываются для всех граждан (и должны быть доступны для всех). Издержки и проблемы интерактивных магнитных карт и мошенничество, связанное с ними, не позволяют считать их идеальным решением в наши дни. Только в США ущерб от мошенничества с кредитными карточками в 1992 г. превысил $1.000.000.000,00, не включая массовое мошенничество с банкоматами. В прошлом не имелось никакой альтернативы, но, к счастью, сегодня смарт-карты предлагают более безопасное и гибкое решение.*

Во всем мире запланировано и осуществляется множество проектов, которые используют "предоплаченные" смарт-карты. Многие из этих карт называются "Городскими Картами" (City Cards), потому что они используются только в том городе, где они выпущены. Городские карты могут выполнять любые функции, от простого применения вместо монет в телефонах, парковочных и продающих автоматах, на общественном транспорте, до сложных систем, позволяющих осуществлять покупки в магазинах без использования наличных денег или кредитных карточек. Большинство людей в настоящее время имеют при себе несколько кредитных карточек, потому что каждый вид обслуживания требует своей карточки. Поскольку смарт-карта может поддерживать различные прикладные системы, то можно выпустить одну смарт-карту, владелец которой просто подписываться на нужные ему услуги. Если кому-либо потребуется в будущем новая услуга, то поддержка ее может добавлена на имеющуюся карту.

*Различие между предоплаченной картой и кредитной карточкой заключается в том, что деньги фактически хранятся на предоплаченной карте. Простейшая предоплаченная карта покупается с записанной на ней некоторой суммой и используется до тех пор, пока все деньги не израсходованы и подобно европейским телефонным карточкам после этого выбрасывается. На более сложных картах сумма денег записывается самим владельцем карты. Это может быть сделано помещением денег в машину, которая затем записывает (переносит) эту сумму в память карты. Таким образом, обычно работают карточки для торговых автоматов, установленных на фирмах для своих сотрудников. По мере расходования денег, владелец может "положить" на карточку дополнительную сумму. Предоплаченные карты обычно называются "денежными" картами.*

Электронные платежи

Будущее финансовых смарт-карт лежит в системе электронных платежей, по-английски называемой Electronic Fund Transfer или EFT. В этих задачах сумма денег помещается на карту непосредственно в банке владельца карты. Как и предоплаченные карты, такие карты могут приниматься магазинами и другими учреждениями наряду с наличными деньгами, но без тех проблем с безопасностью, которые свойственны наличности. Благодаря развитой системе защиты смарт-карта может быть использована только ее владельцем. Эта система безопасности будет описана ниже.

Смарт-карты используются следующим образом. Владелец карты предъявляет свои покупки и карту кассиру. Карта вставляется в специальный кассовый аппарат, по-английски называемый POS (Position of Sale), оборудованный ридером для смарт-карт. Владелец вводит на клавиатуре свой PIN-код (пароль), чтобы подтвердить свое владение карточкой. Ридер проверяет подлинность карты, удостоверяется, что на ней имеется достаточно средств, чтобы оплатить покупку, дебетует карту, кредитует POS-аппарат. И все это осуществляется в считанные секунды! Поскольку деньги и все данные для обеспечения безопасности содержатся на самой карте, нет необходимости в дорогостоящем и отнимающем много времени интерактивном подтверждении каждой транзакции, что обычно производится для магнитных карточек. Деньги перечисляются из кассового аппарата на банковский счет продавца во время одного сеанса телефонной связи с банком в конце рабочего дня. В тех местах, где нет телефонов, деньги могут быть переведены в банк с помощью специальной смарт-карты, на которую записываются данные из POS-аппарата и которая затем относится в банк. При каждом таком переводе денег (как интерактивном, так и с помощью смарт-карты) на кассовом аппарате обновляется список потерянных, украденных и неиспользуемых карт. Карта из такого списка не будет принята для расчета.

*Карты для приобретения* ***бензина*** *на заправочных станциях - другой пример использования смарт-карт. Их польза особенно ощутима для компаний, поскольку последние могут выдавать эти карты водителям всех своих грузовиков. В этом случае все приобретения топлива могут легко контролироваться и фиксироваться. Удобно это и с точки зрения безопасности, т.к. водители и владельцы заправочных станций избавлены от необходимости оперировать большими суммами наличных денег.*

Безопасность.

Поскольку процесс создания смарт-карт достаточно сложен, под силу это только промышленной компании. Во время производства и инициализации карт электронные "предохранители" в микросхеме могут быть разрушены, тем самым предотвращая нежелательное вмешательство в хранимую информацию. Копирование данных, кроме как их производителями, невозможно благодаря уникальному внутреннему коду, записанному на в каждой карте. Даже если данные, записанные на карту, кто-либо сможет продублировать, уникальный внутренний код предотвратит использование карты. При отправке карт производителем в адрес организации, выпускающей карты в обращение, коды посылаются отдельно, так что даже в случае "потери" всей партии, карты останутся непригодными для использования. Пока этот код не будет "представлен" карте, последнюю использовать будет невозможно. Как только карта "выпущена" и в ней записаны данные (или сумма денег), доступ к ним защищается кодированным паролем (или PIN-кодом), известным только хозяину карты. По вашему выбору данные, записанные на карте, могут быть также зашифрованы такими способами, как DES (Стандарт Шифрования Данных), алгоритм которого невозможно нарушить. Все это делает смарт-карты одними из наиболее надежных доступных нам форм хранения данных. При несанкционированной попытке своего использования смарт-карты способны самостоятельно на время или навсегда прекратить свою работу. Например, если личный пароль набирается неправильно трижды, карта автоматически отключается. Для восстановления работоспособности карты необходим ее возврат на место выдачи (обычно это - банк). Если карта утеряна или украдена, ее владелец сообщает о случившемся в банк, и программа банка вносит эту карту в список недействительных карт, рассылаемый на все терминалы продаж (POS). Любая попытка использовать потерянную или украденную карту будет немедленно пресечена. Поскольку все производившиеся трансакции записываются на POS-терминалах и передаются в банк, потерянная или украденная карточка может быть восстановлена с тем же самым количеством денег, которое было на момент ее потери.

Карты контроля доступа используются, чтобы получать физический доступ в здания, комнаты, к автомобильным автостоянкам, загражденным территориям и т.п., а также для получения **логического доступа** к компьютерам или информации, содержащейся в компьютере.

**Карты доступа в помещения** обычно используются теми компаниями, которые хотят ограничить доступ в помещения, а также наблюдать за тем, кто посещает определенные помещения. Служащим компании выдаются смарт-карты, на которых записан уровень доступа, определенный для каждого служащего. Карта может также содержать фотографию, имя, номер владельца (ID) и т.д., нанесенные на поверхности карты. На карте могут быть запрограммированы различные уровни безопасности.

*Для входа на территорию (в дверь, ворота, лифт, и т.д.) служащий должен вставить свою карту в считывающее устройство и набрать свой PIN-код на вспомогательной клавиатуре. В некоторых системах, требующих повышенной защиты, может использоваться также биометрическая информация, например, отпечатки пальцев, характеристики голоса, вид радужной оболочки глаза, которая сравнивается с той информацией, что записана на смарт-карте. Если карта и PIN-код (или биометрические параметры) подлинные, то считывающее устройство посылает сигнал открыть дверь (ворота и т.д.) Обычно дверь удерживается закрытой сильной электромагнитной блокировкой, которую сигнал отключает. Если дверей много, то различные считывающие устройства могут быть соединены с компьютером, который выполняет проверку доступа и посылает сигналы для открытия дверей. Компьютер может также использоваться, чтобы контролировать и сообщать перемещения сотрудников (вход и выход).*

*Бесконтактные карты используются в случае, когда требуется доступ без выполнения каких-либо манипуляций. Если сотрудник носит на одежде такую карту, то при прохождении сотрудника мимо ридера, последний автоматически открывает двери.*

**Карты логического доступа** позволяют управлять доступом к компьютерам и компьютерным сетям. Для доступа к компьютеру пользователь должен вставить смарт-карту в ридер и ввести свой PIN-код. Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Определенный уровень безопасности (доступа) может быть присвоен всем пользователям, группе пользователей, а также отдельным лицам. Смарт-карты управления доступом позволяют реализовать часть или все функции, описанные ниже.

**Контроль входа (log-on access)**. Функции персонального компьютера недоступны пользователю до тех пор, пока он не вставит смарт-карту в ридер и введет свой PIN-код. Система проверяет подлинность карты и подтверждает возможность пользователя иметь доступ к компьютеру. Можно установить, чтобы персональный компьютер автоматически отключался после определенного периода простоя, в случае, если пользователь покидает свое рабочее место, забыв выйти из системы.

**Доступ к устройствам персонального компьютера**. В зависимости от уровня доступа, которым обладает пользователь, доступ может быть ограничен к следующим устройствам персонального компьютера:

* Дисководы гибких дисков, включая защиту от загрузки.
* Накопители на жестких дисках, как локальных, так и сетевых.
* Логические разделы жесткого диска.
* Коммуникационные порты.

**Доступ к программам, файлам и командам.** В зависимости от прав пользователя может контролироваться доступ ко всем или части перечисленных ниже зон системы. "Доступ" может быть далее разбит на права чтения, записи и выполнения, причем возможна любая комбинация из перечисленных прав.

* Операционная система
* Программы и утилиты
* Директории
* Файлы
* Некоторые команды DOS (например, copy, del, fdisk, format, rename и т.д.).

**Контрольные функции.** Возможна регистрация следующих событий:

* Дата и время входа в систему пользователя и выхода из системы
* Допустимые и недопустимые попытки доступа
* Попытки нарушения доступа к ресурсам
* Попытки использовать запрещенные утилиты, программы, команды DOS, и т.д.

**Шифрование данных**, как программное, так и с помощью плат расширения, устанавливаемых в компьютере, может использоваться, чтобы сделать данные недоступными для тех, кто не знает кода дешифровки. Это особенно существенно при передаче важных данных в сети.

***Авторизация программ*** *позволяет запретить выполнение программ, не разрешенных администратором системы. Если программа загружается в систему или выполняется попытка запустить ее с гибкого диска, система предотвращает запуск такой программы, если она не была предварительно разрешена. Процедура разрешения (авторизации) записывает "цифровую подпись" программы. Если после последней авторизации был изменен хоть один бит, такая программа не запустится. Это почти совершенный способ антивирусной защиты, который не требует регулярных обновлений антивирусных программ, что столь обычно при использовании традиционных решений.*

*Многие программные системы защиты предлагают сходные возможности. Существенным отличием является то, что при использовании только программного обеспечения для доступа к системе необходимо всего лишь знать пароль (PIN-код). При использовании решений, основанных на смарт-картах, требуется как знание PIN-кода, так и физическое наличие смарт-карты. Пользователь может и не знать, стал ли его пароль кому-либо известен, но он точно знает, что смарт-карта при нем или утеряна. Кроме того, администратор системы может в любое время запретить доступ к системе любой смарт-карте. Надо отметить, что наибольшие проблемы, связанные с безопасностью компьютерных систем происходят не из-за преднамеренного воровства или разрушения данных (хотя, конечно, и такое случается). Большая часть проблем в защите данных возникает из-за "честных ошибок". Новый пользователь случайно портит или удаляет жизненно важные данные, с компьютерной игрой в систему заносятся вирусы - все это серьезные угрозы для безопасности данных, хранящихся на персональном компьютере или в сети.*

Карты хранения данных используются для хранения информации о здоровье и историй болезни, студенческих зачетных ведомостей, гарантийной или сопроводительной информации и т.д.

Вообще, самый большой потенциал для хранения данных на смарт-картах существует в здравоохранении. Концепция пожизненной карты уже хорошо разработана. Эта карта выдается к человеку при рождении и сохраняется всю жизни. На карте может хранится информация об истории болезней человека, принимаемых лекарствах, рецептах, аллергических реакциях, страховках и т.д. Различные уровни защиты позволять иметь доступ к конфиденциальной информации только тем, у кого есть на это право. Например, аптекарь будет способен просматривать информацию о рецептах заказчика, но не другую, конфиденциальную информацию о здоровье клиента. История болезни пациента легко прослеживается, позволяя быстрый, более точный выбор методов лечения. Поскольку все жизненно важные данные сохраняются на плате, людей, с которыми произошел несчастный случай или болезнь в других городах, можно начинать лечить без необходимости ждать информацию от их лечащего врача. Несколько работающих и экспериментальных версий таких систем уже применяется в США, Европе, и Японии. Результаты показывают, что экономия только на управлении и бумажной работе окупают сами карты, и позволяет больше времени и усилий

Принцип работы смарт-карт на примере транспортных карт Московского метрополитена.

*Итак, речь пойдет о карточках, применяемых в метро, а точнее – об интегральных схемах "MIFARE 1 S50". Сами микросхемы никак с метро не связаны и могут применяться для решения любых задач с бесконтактными ключевыми картами. Тем не менее, для простоты и ввиду причин совершенно очевидных будем ссылаться на них, как на бесконтактные карты метро*.

Сама карта содержит всего два элемента - собственно, микросхему и плоскую обмотку-антенну, используемую как для электропитания карты, так и для связи с хост-системой (турникетом). Наведенное турникетом в антенне напряжение достаточно велико для того, чтобы после выпрямления и стабилизации снабдить карту энергией, необходимой для обработки информации и посылки обратного сигнала. Работает радиосвязь на частоте 13.56 МГц и скорость связи достигает 106 КБод. При этом карта должна находиться на расстоянии никак не более 10 см от турникета. Как правило, для проведения классических операций с картой достаточно 0.1 секунды - за это время можно провести один-два десятка элементарных обменов информацией, таких, как считывание, запись и инкремент блока.

Карта – это один килобайт энергонезависимой памяти. Он делится на 16 секторов по 4 16-байтных блока в каждом. Блок - наименьшая адресуемая единица при работе с картой. Сектор - единица, с которой сопоставляются отдельные права доступа и ключи для проведения операций. Каждый сектор хранит собственную пару ключей, а права доступа указывают, какой доступ при указании какого ключа возможен.

Метро использует только секторы 0 и 15 карты. Нулевой сектор - специальный и в его нулевом блоке хранится уникальный идентификатор карты, который используется для того, чтобы отличать ее от других. В 15, по всей видимости, пишется специфическая для системы информация - к примеру, номер месяца для месячного проездного, число поездок.

Принцип работы. Вы подходите к турникету и подносите карту к датчику. Передающая система датчика наводит в антенне карты электрический ток, который поступает в карту и снабжает ее энергией. Этот же ток несет в себе кодированную информацию запроса турникета к карте. Карта отвечает на него (через туже антенну, используя накопленную энергию) идентификатором, который определяет протокол дальнейшего общения. По идентификатору турникет узнаёт тип карты и "разговаривает" с ней соответственно типу.

Далее идет считывание серийного номера карты. Если в этот момент в поле радиосистемы турникета оказалось более одной карты, происходит коллизия и считывание повторяется до тех пор, пока не будут чисто и без всяких коллизий окажутся, считаны номера всех находящихся в пределах доступности карт. В частности, если в вашем кошельке две карты и лишь одна из них - метрошная, турникет сможет включить лишь ее и попросить остальные карты пока "помолчать". Общение будет происходить с конкретно этой картой.

Затем происходит выбор сектора карты, с которым турникет (или иное устройство для работы с бесконтактными картами) хочет обменяться информацией. Для данного сектора производится обмен шифровками, призванный убедить турникет и карту в том, что они - действительно те, за кого себя выдают. При этом используется способ “я тут дам тебе число, а ты его зашифруй, и ответ пришли мне. А я погляжу, так ли ты зашифровал, как положено”. Эта проверка выполняется с обеих сторон, после чего все уже уверены в том, что они - это они. Включается шифрование канала, и турникет может, в соответствии с разрешенным ему его ключом доступом читать и модифицировать данные в карте.