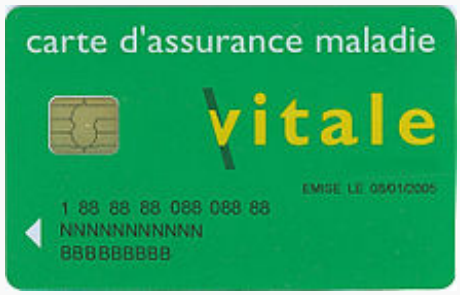
Смарт-карта

ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%B0%D1%80%D1%82%D0%B0

Смарт-карты (англ. *smart card*) — пластиковые карты со встроенной микросхемой (англ. *integrated circuit card, ICC* — карта с интегрированными электронными цепями). В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, управляющую устройством и контролирующую доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления.



Смарт-карта, используемая в системе здравоохранения Франции

Назначение смарт-карт — одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

Смарт-карты находят всё более широкое применение в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов, телефонов стандарта GSM и проездных билетов.

История

Автоматизированная карта со встроенным чипом была изобретена немецким инженером Гельмутом Греттрупом и его коллегой Юргеном Деслофом в 1968 году; патент был окончательно утверждён в 1982 году. Первое массовое использование таких карточек было во Франции для оплаты телефонных счетов, начавшееся в 1983 году.

Французский изобретатель Роланд Морено запатентовал свою первую идею карточки памяти в 1974 году. В 1977 году Мишель Угон из компании Honeywell Bull изобрел первую смарт-карту со встроенным микропроцессором. В 1978 году Honeywell Bull запатентовала СПОМ (самопрограммируемый одночипный микрокомпьютер), который задает необходимую архитектуру, чтобы автоматизировать программирование чипа. 3 года спустя самый первый чип CP8, основанный на этом изобретении, был сделан компанией Motorola. В то время Bull имела 1200 патентов, имеющих отношение к смарт-картам.

В 2001 году Bull продала свою долю CP8 вместе со всеми патентами компании Schlumberger. Впоследствии Schlumberger объединила свой департамент по смарт-картам и CP8 и создала компанию Axalto. В 2006 году компании Axalto и Gemplus, два главных лидера на рынке смарт-карт на то время, объединились и стали называться Gemalto. Второе массовое использование этой технологии с интеграцией микрочипов во все французские дебетовые карты (Carte Bleue) завершилось в 1992 году. При оплате счетов во Франции с использованием Carte Bleue их владельцам нужно было вставить карту в терминал оплаты, затем ввести PIN-код, и потом совершить нужную операцию.

Электронные денежные системы, основанные на технологии смарт-карт, стали активно применяться в Европе в середине 1990-х годов, более значительно в Германии (Geldkarte), Австрии (Quick), Бельгии (Proton), Франции (Moneo), Нидерландах (Chipknip), Швейцарии (Cash), Норвегии (Mondex), Швеции (Cash), Финляндии (Avant), Великобритании (Mondex), Дании (Danmønt) и Португалии (Porta-moedas Multibanco).

Наибольший подъём в использовании смарт-карт пришелся на 1990-е годы, с введением SIM-карт, основанных на смарт-картах, в аппараты мобильных телефонов GSM в Европе. С распространением мобильных телефонов в Европе смарт-карты также стали повсеместными.

Международные платёжные системы MasterCard, Visa и Europay в 1993 году подписали соглашение о совместной работе, чтобы развить технические характеристики для использования смарт-карт при оплате счетов кредитными и дебетовыми картами. Первая версия систем стандарта EMV (Europay, MasterCard, Visa) была выпущена в 1994 году. В 1998 году стала доступна следующая версия технических характеристик.

Повсеместно, за исключением некоторых стран, например, США, наблюдался значительный прогресс в использовании совместимого с EMV оборудования в торговых точках и в выпуске дебетовых и кредитных карт с техническими характеристиками, соответствующими стандарту EMV. Обычно национальные платёжные ассоциации, при участии и поддержке компаний MasterCard International, Visa International, American Express и JCB, постепенно выполняли план, согласованный со всеми вовлечёнными в это заинтересованными сторонами.

Для банков, заинтересованных во внедрении смарт-карт, единственный плюс, поддающийся количественному определению, — это возможность значительного снижения подделок. Некоторые критики утверждают, что сбережения намного меньше, чем стоимость внедрения EMV, и поэтому многие думают, что платёжные системы США предпочитают переждать текущий цикл EMV, чтобы потом внедрить новую, бесконтактную технологию.

Смарт-карта с бесконтактным интерфейсом становится все более популярной для оплаты счетов и проезда в общественном транспорте. Visa и MasterCard подписали соглашение на простую в реализации версию, которая была введена в использование в США в 2004—2006 годах. По всему миру были внедрены бесконтактные системы сбора оплаты за проезд в общественном транспорте. Различные развивающиеся стандарты при близком рассмотрении несовместимы, хотя бесконтактная технология Mifare от компании Philips имеет существенную долю в торговле в США и Европе.

Смарт-карты также были внедрены в идентификацию личности и документацию на региональном, национальном и международном уровне, это гражданские карточки, водительские права и медицинские документы. В Малайзии карточки удостоверения личности MyKad, включающие в себя 8 различных функций, есть у 18 миллионов жителей. Бесконтактные смарт-карты внедряются в биометрические паспорта, чтобы увеличить уровень безопасности в международных поездках.

Виды смарт-карт

Все смарт-карты можно разделить по способу обмена со считывающим устройством на:

- контактные смарт-карты с интерфейсом ISO 7816;
- контактные смарт-карты с USB-интерфейсом;
- бесконтактные (RFID) смарт-карты.

Существуют карты, которые включают в себя как контактные, так и бесконтактные интерфейсы.

По функциональности карты можно разделить на

- карты памяти (содержат некоторое количество данных и механизм разграничения доступа к ним)
- интеллектуальные карты (содержат микропроцессор и возможность управлять данными на карте)

Контактные смарт-карты с интерфейсом ISO 7816

Контактные смарт-карты имеют зону соприкосновения, содержащую несколько небольших контактных лепестков. Когда карта вставляется в считыватель, чип соприкасается с электрическими коннекторами, и считыватель может считать и/или записать информацию с чипа.

Форма карты, контактов, их расположение и назначение регламентируются в стандартах ISO/IEC 7816 и ISO/IEC 7810. Стандарт ISO/IEC 7816 регламентирует также протоколы обмена и некоторые аспекты

работы с данными, которые используются и для других смарт-карт.

Контактные карты не содержат батареек; энергия подается считывателями.

Наиболее массовые контактные смарткарты — это SIM-карты сотовой связи, таксофонные карты, современные банковские карточки.

Контактные смарт-карты с USB-интерфейсом

Обычно представляют собой микросхему обычной ISO 7816 карты, совмещенную с USB-считывателем в одном миниатюрном корпусе. Это делает применение смарт-карт для компьютерной аутентификации гораздо удобнее.

Пример — изделия Rutoken и eToken.

Бесконтактные смарт-карты

Бесконтактные смарт-карты — карты, в которых карта общается со считывателем с помощью технологии RFID. Требуется подносить карточки достаточно близко к считывателю, чтобы провести необходимые операции. Они часто применяются в областях, где необходимо провести операцию быстро, например, в общественном транспорте.

Стандарт для бесконтактных смарт-карт — ISO/IEC 14443, реже ISO/IEC 15693.

Для работы с бесконтактными смарт-картами применяется технология RFID. Как и контактные смарт-карты, бесконтактные не имеют батареек. В них встроена катушка индуктивности, чтобы запасти энергию для начального радиочастотного импульса, который затем выпрямляется и используется для работы карточки.

Примеры широко используемых бесконтактных смарт-карт — это проездные в метрополитене и наземном транспорте, электронные («биометрические») паспорта, некоторые виды карт в системах контроля доступа (СКУД).

Карты памяти

Содержат некоторое количество данных и фиксированный механизм разграничения доступа к ним. Как правило, это карты для микроплатежей на транспорте, таксофонах, в парках отдыха, карты лояльности клиентов и т. п.

В качестве механизма ограничения доступа могут выступать как очень простые (однократная запись, пароль, уникальный номер), так и посложнее (взаимная аутентификация с использованием стандартных симметричных криптоалгоритмов AES, DES).

Карты памяти — наиболее распространенные смарт-карты (проездные в метрополитене и наземном транспорте, таксофонные карты).

Интеллектуальные карты

Содержат микропроцессор и возможность загружать алгоритмы его работы. Возможные действия таких карт включают в себя комплексные действия при аутентификации, сложные протоколы обмена, регистрация фактов доступа и т. п.

Помимо симметричной криптографии (AES, DES), знают асимметричную (RSA), алгоритмы инфраструктуры открытых ключей (PKI), имеют аппаратные генераторы случайных чисел, усиленную защиту от физической атаки.

Как правило, функционируют под управлением операционной системы (например, JCOP или MULTOS) и

снабжены соответствующим пакетом сертификатов.

Примеры — электронные («биометрические») паспорта и визы, SIM-карты.

Считыватели для контактных смарт-карт

Несмотря на название — устройство для чтения смарт-карт, большинство оконечных устройств, или устройств сопряжения (IFD, InterFace Device), способны как считывать, так и записывать, если позволяют возможности смарт-карты и права доступа. Устройства для чтения смарт-карт могут подключаться к компьютеру посредством:

Устройства чтения смарт-карт могут быть интегрированы в клавиатуру.

Некоторые производители выпускают другие виды аппаратных устройств, представляющие собой интеграцию контактной смарт-карты с устройством чтения смарт-карты. Они по свойствам памяти и вычислительным возможностям полностью аналогичны смарт-картам. Наиболее популярны аппаратные «ключи», использующие порт USB. USB-ключи привлекательны для некоторых организаций, поскольку USB становится стандартом, находящим всё большее распространение в новых компьютерах: организации не нужно приобретать для пользователей какие бы то ни было считыватели.

Использование интеллектуальных устройств при аутентификации с открытым ключом

Смарт-карты, USB-ключи и другие интеллектуальные устройства могут повысить надёжность служб PKI: смарт-карта может использоваться для безопасного хранения закрытых ключей пользователя, а также для безопасного выполнения криптографических преобразований. Безусловно, интеллектуальные устройства аутентификации не обеспечивают абсолютную защиту, но их защита намного превосходит возможности обычного настольного компьютера.

Хранить и использовать закрытый ключ можно по-разному, и разные разработчики используют различные подходы. Наиболее простой из них — использование интеллектуального устройства в качестве дискеты: при необходимости карта экспортирует закрытый ключ, и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, зато относительно легко реализуемым и предъявляющим невысокие требования к интеллектуальному устройству.

Два других подхода более безопасны, поскольку предполагают выполнение интеллектуальным устройством криптографических операций. При первом пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства. При втором пользователь генерирует ключи при помощи устройства. В обоих случаях, после того как закрытый ключ сохранён, его нельзя извлечь из устройства и получить любым другим способом.

Генерирование ключевых пар

В случае генерирования ключа вне устройства пользователь может сделать резервную копию закрытого ключа. Если устройство выйдет из строя, будет потеряно, повреждено или уничтожено, пользователь сможет сохранить тот же закрытый ключ на новой карте. Это необходимо, если пользователю требуется расшифровать какие-либо данные, сообщения, и т. д., зашифрованные с помощью соответствующего открытого ключа, но это кратковременные проблемы в обеспечении аутентификации. Кроме того, при этом закрытый ключ пользователя подвергается риску быть похищенным.

В случае генерирования ключа с помощью устройства закрытый ключ не появляется в открытом виде, и нет риска, что злоумышленник украдёт его резервную копию. Единственный способ использования

закрытого ключа — это обладание интеллектуальным устройством. Являясь наиболее безопасным, это решение выдвигает высокие требования к возможностям интеллектуального устройства: оно должно генерировать ключи и осуществлять криптографические преобразования. Это решение также предполагает, что закрытый ключ не может быть восстановлен в случае выхода устройства из строя, и т. п. Об этом необходимо беспокоиться при использовании закрытого ключа для шифрования, но не там, где он используется для аутентификации или в других службах, где используется цифровая подпись.

Применение

Компьютерная безопасность

Некоторые системы дискового шифрования, такие, как FreeOTFE, TrueCrypt и Microsoft Windows 7BitLocker, могут использовать смарт-карты для безопасного хранения ключей и также для добавления дополнительного уровня шифрования для критичных частей на защищаемом диске. Смарт-карты также используются для единого входа в систему.

Применения в финансовой сфере

Приложения смарт-карт включают их использование в банковских, дисконтных, телефонных карточках и карточках оплаты проезда, различных бытовых услуг и т. д.

Смарт-карты также могут использоваться как электронные кошельки. На чип смарт-карты может быть загружена информация о средствах, которыми владелец может расплачиваться в различных торговых точках (см. карта с хранимой стоимостью).

Криптографические протоколы защищают информационный обмен между смарт-картой и банкоматом.

Если при этом нет непосредственной связи с банком, то работа с картой проходит в режиме off-line, в отличие от магнитных карт, которые делают запрос в банк, и уже он дает разрешение на операции с картой.

Идентификация

Быстро развивается применение смарт-карт в цифровой идентификации. В этой сфере карты используются для удостоверения личности. Более общий пример — это конъюнкция с PKI. Смарт-карта сохраняет зашифрованный цифровой сертификат, полученный от PKI вместе с некоторой другой информацией о владельце.

При совмещении подобных смарт-карт с биометрическими данными получается двух- или трехфакторная аутентификация.

Первая система водительских прав, основанная на смарт-картах, была введена в провинции Мендоса в Аргентине. Там был высокий уровень аварий на дорогах и низкий уровень по оплате штрафов. Смарт-права отвечали современным требованиям записей нарушений правил и неоплаченных штрафов. Они также содержали личную информацию водителя, его фотографию, и по желанию владельца медицинскую информацию. Правительство ожидало, что новая система поможет собрать более 10 млн $ за штрафы.

К началу 2009 года все население Испании и Бельгии имело eID-карты, которые были выданы правительством и использовались для удостоверения личности. Эти карточки содержат 2 сертификата: один — для аутентификации, другой — для подписи. Все больше услуг в этих странах используют eID-карты для авторизации.

С 2010 года в Российской Федерации начато внедрение универсальной электронной карты в качестве средства идентификации.

Цифровое телевидение

Ресивер цифрового телевидения и карта доступа

Смарт-карты (карты условного доступа) широко используются для активации закодированных телеканалов платного цифрового эфирного, спутникового и кабельного телевидения.

Применяются в различных системах условного доступа.

Микросхема карты не только осуществляет часть декодирования сигнала, но и содержит индивидуальный номер (ID) абонента, что позволяет оператору цифрового телевидения управлять доступом. Когда подписка у абонента заканчивается, оператор включает в поток кодированного видеосигнала дополнительные управляющие команды, получив которые, карта доступа этого абонента блокирует просмотр кодированных телеканалов. После оплаты подписки по той же схеме доступ к кодированным каналам возобновляется.

Используется большинством операторов спутникового телевидения, например: «НТВ-Плюс», кодировка Viaccess; «Континент ТВ» и «Радуга ТВ», кодировка Irdeto; «Телекарта ТВ», кодировка Conax; «Триколор ТВ», кодировка DRE-Crypt.

Безопасность

Стандарты

Вопросы безопасности смарт-карт регулируются большим количеством интернациональных и фирменных стандартов и правил. Особняком можно выделить государственные законы, регулирующие: экспорт/импорт оборудования и алгоритмов цифровой безопасности; правила цифровой безопасности в государственных структурах.

Наиболее известны следующие стандарты:

- ISO/IEC 15408, более известный как Common Criteria — широкий свод правил, относящихся к безопасности цифровых систем.
- Federal Information Processing Standards (FIPS). Национальные стандарты США в области информационной безопасности. Применительно к безопасности смарт-карт наиболее известен FIPS-140 — требования к криптографическим механизмам.
- EMV — совместный стандарт Europay, MasterCard и VISA для карточных платежных систем.

Вопросы безопасности зачастую входят в отраслевые стандарты, например, GlobalPlatform, EPC, JavaCard, и т. д.

Методы атаки на смарт-карты[1]

- Поиск уязвимостей криптоалгоритмов смарт-карт. Этому способствует практически полная открытость всех используемых алгоритмов. Однако найденные уязвимости быстро устраняются.
- Дифференциальный анализ питания — оценка осциллограмм потребляемой смарт-картой электроэнергии в момент выполнения криптоалгоритма.
- Физический взлом — получение доступа к электрическим цепям смарт-карты после химического снятия защитных слоев с кристалла. Позволяет провести анализ устройства смарт-карты и подключиться к ней с помощью микроэлектродов.
- Необычные условия эксплуатации смарт-карт. Например, нештатный температурный режим, напряжения и частоты сигнала на контактах и т. д. Это может приводить к сбоям в алгоритмах с последующим получением доступа к информации.

Проблемы

- Возможный отказ. Пластиковая карта в ходе эксплуатации испытывает значительные деформационные воздействия, что влечет повышение вероятности излома чипа. Однако у крупных банковских систем затраты, связанные с отказами смарт-карт, компенсируют возможные затраты, связанные с мошенничеством.
- Использование смарт-карт в общественном транспорте представляет собой угрозу для конфиденциальности, потому что такая система дает возможность третьим лицам следить за передвижением владельцев карт.
- Использование смарт-карт для идентификации и аутентификации владельца — это наиболее безопасный способ для банковских интернет-приложений, но безопасность все равно не полная. Если на компьютер установлено вредоносное ПО, то безопасное выполнение интернет-приложений не гарантировано. Например, это ПО может незаметно для владельца изменить операции. Пример подобного ПО — троян Silent Banker. Некоторые банки (Fortis и Dexia в Бельгии) дополняют свои смарт-карты бесконтактным считывателем; владелец делает запрос на сайте банка, вводя свой PIN-код, желаемую операцию и цифровую подпись, полученную от считывателя, и эта подпись сравнивается банком.
- Проблема нехватки стандартов для смарт-карт. Для решения этой проблемы был запущен проект ERIDANE, который занимается разработкой новой структуры смарт-карт, которые будут работать на оборудовании Point Of Interaction (POI).

Тенденции развития

- Расширение коммуникационных возможностей карты.
- Реализация многозадачного режима работы — возможности одновременно выполнять несколько приложений[2].

Примечания

1. ↑ Практически все методы атаки учитываются при проектировании и тестировании смарткарт, а также учтены в соответствующих стандартах.
2. ↑ Голдовский И. М., 2010, с. 182.

Литература

- *И. М. Голдовский.* Банковские микропроцессорные карты. — М.: «Альпина Паблишер», 2010. — 694 с. — (Библиотека Центра исследований платежных систем и расчетов). — ISBN 978-5-9614-1233-8.