Оглавление

Предисловие

Основная идея этой книги принадлежит Владимиру Федоровичу Шаньгину – доктору технических наук, заслуженному профессору Национального исследовательского университета МИЭТ, лауреату Государственной премии СССР, действительному члену Международной академии информатизации и автору целой серии известных в профессиональной среде монографий, посвященных различным аспектам информационной безопасности.

Несмотря на достаточно большое количество публикуемых книг схожей тематики, не получили широкой известности монографии, посвященные именно вопросам сосуществования технологий защиты информации и смарт-технологий. Тогда как они, без сомнения, успешно дополняют друг друга и в очень многих случаях используются совместно:

- методы и средства защиты информации активно применяются в мире смарт-карт: непосредственно в смарт-картах и в использующих их приложениях;
- и наоборот, смарт-карты нередко используются в средствах обеспечения информационной безопасности.

Таким образом, было решено, что книга «Смарт-карты и информационная безопасность» будет актуальна и востребована среди книг со схожей тематикой. Для работы по созданию книги В. Ф. Шаньгин пригласил нас, ее авторов:

- *Константина Яковлевича Мытника*, начальника отдела смарт-карт НИИ Молекулярной Электроники (НИИМЭ), лауреата Премии Правительства РФ, 20 лет работающего в области смарт-технологий;
- *Сергея Петровича Панасенко*, кандидата технических наук, заместителя генерального директора Фирмы «АНКАД» – одной из ведущих отечественных компаний-разработчиков средств защиты информации.

Авторы книги являются также членами ряда рабочих групп Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26). Выбор авторов был обусловлен тем, что именно технологии смарт-карт и защиты информации, а также их совместного использования являются направлениями их повседневной профессиональной деятельности.

Книга адресована специалистам в области информационных технологий и информационной безопасности, желающим эффективно использовать смарт-технологии в своей деятельности. Не секрет, что смарт-технологии стали важным инструментом обеспечения информационной безопасно-

сти (ИБ) в современных системах массового обслуживания, и необходимо научиться применять его грамотно. Наша книга – попытка взглянуть на смарт-технологии через призму ИБ.

Мы стремились сделать смарт-технологии понятнее и доступнее читателю. Для этого мы соединили в одной книге информацию об устройстве и возможностях смарт-карт, основы криптографии, примеры реальных приложений и вводный курс в разработку собственных приложений для смарт-карт.

Авторы намерены поддерживать сайт книги www.sc-is.ru, на котором будут доступны некоторые упоминаемые в тексте инструментальные средства, а также актуальный список исправлений.

Книга состоит из ряда тематических частей, каждая из которых включает в себя несколько логически связанных глав.

Первая часть содержит обзор основ смарт-технологий:

- *глава 1* вводит читателя в мир смарт-технологий, в ней дается обзор основных сфер применения смарт-карт и краткий экскурс в историю;
- *глава 2* предлагает взгляд на смарт-карту «изнутри», представляя типичную конструкцию смарт-карты, ее аппаратное и программное обеспечение;
- *глава 3* важна для дальнейшего понимания всего содержания книги; она содержит описание основных функций смарт-карты, включая протоколы обмена карты с «внешним миром», базовый набор команд взаимодействия со смарт-картой, принципы организации данных на карте и порядок разграничения доступа к хранящейся на ней информации.

Вторая часть книги рассказывает об основных криптографических алгоритмах и протоколах:

- *глава 4* дает основные понятия и определения в данной области и подробно описывает алгоритмы шифрования данных;
- *глава 5* посвящена основным методам обеспечения целостности данных: алгоритмам хеширования и электронной подписи;
- *в главе 6* рассмотрены механизмы работы с криптографическими ключами, в ней подробно описаны основные аспекты генерации и использования ключей;
- *глава 7* описывает ряд методов и протоколов аутентификации.

Третья часть посвящена спецификациям, описывающим вопросы взаимодействия со смарт-картами на различных уровнях:

- *глава 8* рассказывает о семействе спецификаций PC/SC;

- *глава 9* рассматривает вопросы управления приложениями согласно спецификации Global Platform.

Четвертая часть подробно описывает ряд примеров конкретных приложений с целью иллюстрации теоретического материала предыдущих частей книги:

- *глава 10* представляет реализацию приложения «Домен безопасности»;
- *глава 11* показывает возможности и характеристики средства криптографической защиты информации, основанного на микросхеме смарт-карты;
- *глава 12* рассматривает применение смарт-карт в качестве электронных идентификационных документов на примере загранпаспорта;
- *глава 13* описывает использование платежных карт на основе международной спецификации EMV; отдельный раздел данной главы посвящен отечественной платежной карте МИР.

Пятая часть книги посвящена технологиям JavaCard и предоставляемым ими возможностям по созданию приложений для смарт-карт:

- *глава 14* рассматривает особенности языка программирования JavaCard и описывает основные возможности по работе с апплетами;
- *глава 15* дает подробный обзор библиотек для разработки приложений для смарт-карт;
- заключительная глава книги – *глава 16* – предлагает читателю примеры апплетов для смарт-карт на основе технологий JavaCard; отдельный раздел главы дает рекомендации программистам по созданию эффективных приложений для смарт-карт.

Книга снабжена рядом приложений, в которые вынесена полезная информация, не нашедшая своего места на страницах основных частей книги:

- *Приложение А* содержит информацию об интернет-сайте книги – www.sc-is.ru;
- *Приложение Б* описывает работу утилиты Smacon – интерпретатора команд для смарт-карт, который можно скачать с сайта книги;
- *Приложение В* посвящено описанию формата TLV, широко применяемого в технологиях смарт-карт и криптографии;
- *Приложения Г и Д* содержат таблицы рассмотренных в основной части книги отечественных стандартов шифрования и хеширования.

Кроме того, в заключительной части книги читатель сможет найти англо-русский словарь терминов в области смарт-карт и список используемых в книге сокращений.

Авторы будут признательны читателям за любые замечания по нашей книге, в том числе критические. Ждем ваших писем по адресам электронной почты komytnik@niime.ru и serg@panasenko.ru.

Благодарности

Прежде всего, авторам хотелось бы высказать огромную благодарность Владимиру Федоровичу Шаньгину как за идею написания книги «Смарт-карты и информационная безопасность», так и за множество советов и рекомендаций по ее созданию и по материалу, который был включен в книгу. Не будет преувеличением утверждать, что без конструктивного руководящего участия Владимира Федоровича данная книга не увидела бы своего читателя.

Авторы выражают глубокую признательность всему коллективу отдела смарт-карт зеленоградского института НИИМЭ. Накопленный им опыт в значительной мере послужил основой этой книги. Многие сотрудники любезно согласились ознакомиться с черновиками книги, поправили ошибки и высказали чрезвычайно полезные замечания по ее содержанию. Хотелось бы персонально поблагодарить разработчика утилиты Smacon Владимира Сергеева, Андрея Степанова за особенно ценные замечания по JavaCard и главного автора «визарда команд» Ирину Попову.

Авторы также благодарны сотрудникам Фирмы «АНКАД», внесшим свой вклад в создание книги, среди которых стоит особенно отметить Ирину Любушкину и Дмитрия Тюфякина.

Кроме того, авторы признательны Олегу Тараскину (Bankex Foundation) и Сергею Петренко (Университет Иннополис) за ряд ценных рекомендаций и замечаний по книге в целом и представленному в ней материалу.

Часть I

Мир смарт-карт

Глава 1

Знакомство со смарт-картами

Мы сталкиваемся со смарт-картами в своей повседневной жизни, когда расплачиваемся картой в магазине, предъявляем загранпаспорт на пункте паспортного контроля при выезде за рубеж или когда разговариваем по мобильному телефону.

К «смарт-картам» можно также отнести устройства, исполненные в других форм-факторах, но предназначенные для обеспечения информационной безопасности и построенные на основе аналогичных микросхем. Например, SIM-карты мобильных телефонов, инлеи (пластиковые страницы с интегрированной антенной) электронных документов, криптографические USB-токены и т. п.

Актуальность проблем информационной безопасности в современном мире стимулирует распространение смарт-технологий на новые рынки: *элементы безопасности* смартфонов, планшетов и других мобильных устройств; интернет вещей; промышленные автоматические системы и пр. Вполне вероятно, что через несколько лет с момента написания книги смарт-карты найдут применение в областях, о которых мы сейчас даже не подозреваем.

Несмотря на постоянное развитие аппаратного обеспечения и появление новых идей применения смарт-карт, основные принципы их устройства и функционирования остаются актуальными. Надеемся, что изложенный в книге материал будет полезен читателям в их сегодняшней деятельности и послужит подспорьем для дальнейшего развития.

1.1. Основные понятия

Смарт-карты – это защищенные микроэлектронные устройства, предназначенные для обеспечения информационной безопасности. Задачи смарт-карт в современном мире очень разнообразны, но их главное назначение – защита информации.

Под *смарт-технологиями* понимают информационные технологии, ключевым элементом которых является «смарт-карта» в расширительном толковании этого термина.

Смарт-карта всегда взаимодействует с некоторым устройством, которое мы для простоты будем называть *терминалом*. Терминал обязательно

включает контактный или бесконтактный *считыватель*, отвечающий за непосредственный обмен данными с картой на низком уровне, и управляющий модуль, реализующий логику того или иного приложения. Встречаются разнообразные конфигурации терминалов, приведем лишь несколько примеров для иллюстрации:

- интегрированный платежный терминал в магазине, представляющий собой автономное устройство со встроенным считывателем;
- терминал обслуживания транспортных карт, включающий персональный компьютер и подключенный к нему проводом считыватель, реализованный в виде отдельного устройства;
- виртуальный (или удаленный) терминал, состоящий из смартфона пользователя с поддержкой протокола NFC для обмена данными с картой и «облачного» управляющего модуля.

Организацию, отвечающую за выпуск смарт-карты, называют ***эмитентом***. В сферу компетенции эмитента входит внешний вид карты, а также управление приложениями и общими ресурсами на карте. Смарт-карта может содержать несколько приложений, принадлежащих нескольким организациям – *провайдерам приложений*. Эмитент организует взаимодействие провайдеров приложений между собой и обеспечивает безопасный доступ приложений к общим ресурсам.

К основным функциям смарт-карт относятся:

- безопасное *хранение* конфиденциальной информации владельца;
- безопасное *предоставление* конфиденциальной информации владельца уполномоченным контрагентам (платежным терминалам, валидаторам на транспорте, автоматизированным системам паспортного контроля и т. п.);
- выполнение криптографических операций в интересах владельца.

Смарт-карта обязана обеспечить доступ к информации только уполномоченным субъектам. То есть субъекты доступа должны быть аутентифицированы. Аутентификация пользователей, к числу которых относится и владелец смарт-карты, осуществляется путем проверки ПИН'а или биометрических параметров, обычно отпечатка пальца. Полномочия автоматизированных систем (АС), осуществляющих доступ к данным на карте, доказываются наличием у АС определенного секрета – криптографического ключа. Аутентификация АС может быть основана на симметричной или асимметричной криптографической схеме.

Часто для осуществления доступа к смарт-карте требуется *многофакторная аутентификация* – одновременное проведение нескольких видов аутентификации, например, проверка ПИН'а пользователя вместе с аутентификацией терминала.

Для доступа к отдельным элементам данных на карте необходимы различные полномочия. Например, версия приложения может быть доступна без ограничений, тогда как для чтения фамилии владельца карты требуется предъявление ПИН'а, а для обновления персональных данных владельца карты необходима многофакторная аутентификация . Поэтому данные на карте обычно располагаются в файлах, имеющих атрибуты доступа, которые определяют условия осуществления каждого вида доступа, наподобие того, как это устроено в ОС Linux или Windows.

Карта должна обеспечить безопасное предоставление информации. Для этого используется защищенный канал обмена с терминалом, который обеспечивает целостность, конфиденциальность и аутентичность передаваемых данных.

Особая миссия смарт-карты заключается в хранении криптографических ключей и выполнении криптографических операций в интересах владельца карты и провайдера приложения. Симметричные ключи и секретные части ключевых пар являются неизвлекаемыми. Обычно карты обеспечивают возможность генерации асимметричной ключевой пары внутри микросхемы без какой бы то ни было возможности выдачи секретной части ключа наружу.

Смарт-карты часто играют роль персонального модуля безопасности своего владельца. Например, они используются для генерации квалифицированной электронной подписи (ЭП) или удаленной аутентификации владельца в информационной системе.

1.2. Сферы применения смарт-карт

Смарт-карты давно и прочно вошли в наш быт (рис. 1.1). Каждый из нас, порывшись в собственном кошельке и карманах, извлечет несколько образцов различных смарт-устройств в виде пластиковых карт, электронных документов или брелоков. Еще одна карта наверняка находится внутри вашего мобильного телефона или планшета.

Давайте пройдемся по основным сферам применения смарт-карт.

1.2.1. *Платежные карты*

Подавляющее большинство выпускаемых ныне платежных карт имеют встроенную микросхему, обеспечивающую несоизмеримо более высокий уровень безопасности по сравнению со старыми картами с магнитной полосой. Все большее распространение получают платежные карты с радио-интерфейсом. Они позволяют моментально совершать платежи на небольшие суммы – достаточно просто приложить карту к терминалу.

Индустриальным стандартом в области платежных карт является спецификация EMV, которая издается и поддерживается компанией EMVCo (см. [64]). EMVCo образована крупнейшими платежными системами VISA

и MasterCard, к которым присоединились UnionPay (национальная китайская платежная система), American Express, JCB и Discover. Ассоциированными членами EMVCo являются множество технологических компаний и национальных платежных систем, включая Российскую платежную систему МИР.

Рис. 1.1. Сферы применения смарт-карт

Спецификации EMV регламентируют многие аспекты индустрии, включая требования к смарт-картам и терминалам, технологию персонализации и, что очень важно, процедуры сертификации смарт-карт и терминалов.

Платежные системы выпускают собственные спецификации на основе EMV. Совместимость с EMV гарантирует техническую интероперабельность смарт-карт различных платежных систем и терминального оборудования, обеспечивающего прием этих карт. Помимо общих спецификаций, EMVCo выпустила открытую, полностью завершенную спецификацию платежного приложения CPA (Common Payment Application), которая реализуется непосредственно или берется за основу многими разработчиками собственных платежных приложений.

Российское приложение МИР тоже основывается на спецификации EMV, добавляя ряд полезных расширений, позволяющих использовать банковские карты для нефинансовых применений. В частности, приложение поддерживает взаимную аутентификацию и защищенный канал обмена с локальным или удаленным терминалом. Поддержка радио-интерфейса и жесткие требования к длительности транзакции по бесконтактному интерфейсу (не более 0,4 сек.) позволяют использовать приложение даже в

системах СКУД (управление доступом) и на транспорте. Политика оператора платежной системы МИР – компании «НСПК» – направлена на максимальное распространение нефинансовых сервисов с использованием платежных карт МИР.

1.2.2. *Электронные документы*

Все большее распространение во всем мире получают электронные документы. После террористической атаки 2001 года на башни-близнецы в Нью-Йорке правительства всего мира озаботились повышением уровня безопасности паспортно-визовых документов. Теперь загранпаспорта практически всех стран мира оснащаются микросхемами. В РФ электронные загранпаспорта выпускаются уже более 10 лет. Многие европейские страны от Германии до Эстонии внедрили национальные системы идентификации граждан на основе ID-карт. Благодаря этому все больше операций по взаимодействию гражданина с правительством проводится удаленно, вплоть до голосования на выборах в Эстонии.

Особую категорию составляют социальные и муниципальные карты. К ним предъявляются менее жесткие требования по безопасности, но сценарии использования роднят их с другими электронными документами. В Европе большой популярностью пользуются электронные медицинские карты, которые иногда выделяют в самостоятельное направление смарт-технологий.

Россия тоже движется в направлении внедрения электронных документов. Для иллюстрации приведем далеко не исчерпывающий список российских проектов в этой области, демонстрирующий масштаб проникновения электронных документов в нашу жизнь (табл 1.1).

Таблица 1.1. Российские электронные документы

Проект	Состояние
Биометрический загранпаспорт	Действует
Универсальная Электронная Карта (УЭК)	Закрыт
Карта москвича	Действует
Карта жителя Татарстана	Действует
Электронный полис ОМС	Действует
Карта водителя для цифрового тахографа	Действует
Карта военнослужащего	Действует
Удостоверение личности гражданина РФ	Стартует
Электронное водительское удостоверение	Стартует
Электронное свидетельство о регистрации транспортного средства	Стартует

1.2.3. *Транспортные карты*

Смарт-карты давно стали привычным атрибутом транспортных систем больших городов по всему миру. Одним из крупнейших в мире пользователей транспортных карт является Московский метрополитен.

Транспортные карты работают по радио-интерфейсу. Большинство из них представляют собой простейшие микросхемы с аппаратно реализованной жесткой логикой, однако все чаще встречаются программно-управляемые смарт-карты, которые обеспечивают более высокий уровень функциональности и безопасности, а также возможность размещать на таких картах дополнительные приложения, например, социальное или дисконтное.

Среди транспортных систем практикуются два подхода к обеспечению безопасности. Одни делают ставку на обработку операций с использованием черного списка фальшивых карт. В этом случае от самой карты требуется только хранение уникального идентификатора и электронной подписи, подтверждающей ее аутентичность. Защита от клонирования и перерасхода основана на контроле в режиме онлайн.

Другие транспортные системы делают акцент на защите микросхемы смарт-карты, которая гарантирует безопасность проведения операции и защиту от клонирования. Защищенные карты несколько дороже, но позволяют безопасно проводить операции в автономном режиме, работать без объемного черного списка и экономить на связи.

Самыми распространенными транспортными картами в мире, лидирующими по объему выпуска с огромным отрывом, являются карты семейства Mifare, выпускаемые компанией NXP, или их клоны. Для иллюстрации приведем технические характеристики некоторых членов семейства (табл. 1.2).

Таблица 1.2. Характеристики карт семейства Mifare

Карта	Объем памяти	Криптографические алгоритмы
Ultralight	64 байта	–
Ultralight C	192 байта	3DES
Mifare Classic	1K–4K	Crypto1
Mifare Plus	2K–4K	Crypto1, AES-128

Несмотря на популярность карт Mifare, давно заметны их недостатки, многие из которых обусловлены историческими причинами. Среди главных проблем: неполное соответствие протокола Mifare международному стандарту ISO 14443, отсутствие файловой системы, низкий уровень информационной безопасности карт, использующих старый криптографический алгоритм Crypto1. Ряд компаний, работающих в сфере транспорта

и смежных областях, объединились в альянс (OSPT Alliance – см. [61]) и выпустили современную спецификацию транспортной карты Cipurse, основанную на многолетнем опыте практической работы и лишенную известных недостатков семейства карт Mifare. Существуют еще несколько крупных транспортных проектов, например, европейские карты Calypso (см. [60]).

1.2.4. *СКУД*

Смарт-карты широко применяются в качестве пропусков в различных организациях, на промышленных предприятиях, в учреждениях, отелях и даже школах. Автоматические системы контроля и управления доступом сокращенно называют СКУД. Смарт-карты доказали свою эффективность в этой области и получают все большее распространение.

Смарт-карты или токены также используются для разграничения доступа к компьютерной технике.

Карты для СКУД во многом похожи на транспортные карты, но требования к их безопасности более высокие.

1.2.5. *Телекоммуникации (SIM-карты)*

SIM-карты хорошо знакомы всем. Количество выпущенных в мире SIM-карт ныне превосходит население планеты. SIM-карты можно найти не только в мобильных телефонах, но и в планшетах, навигаторах и других устройствах, подключаемых к Интернету.

Микросхемы для SIM-карт характеризуются умеренными требованиями к безопасности и высокими требованиями к функциональности. Большинство из них имеют встроенную виртуальную машину, обеспечивающую гибкое управление приложениями в процессе эксплуатации.

1.2.6. *Модули безопасности*

Одно из перспективных направлений смарт-технологий – создание высокозащищенных микросхем для обеспечения защиты информации в открытых средах. Вот некоторые примеры:

- *Криптографический токен* с USB-интерфейсом для защиты информации на личном компьютере пользователя. Токен содержит защищенную от инженерного взлома микросхему и не подвержен атакам вредоносного ПО. Он обеспечивает безопасную генерацию ЭП пользователя, аутентификацию пользователя при доступе к удаленным сервисам, выработку сессионных ключей и другие необходимые криптографические операции.
- *Элемент безопасности* (ЭБ) мобильного устройства отвечает за безопасное хранение ключей и выполнение криптографических опера-