

Оглавление

Предисловие.....	11
Благодарности.....	14
Часть I. Мир смарт-карт.....	15
Глава 1. Знакомство со смарт-картами.....	16
1.1. Основные понятия	16
1.2. Сферы применения смарт-карт.....	18
1.2.1. Платежные карты	18
1.2.2. Электронные документы.....	20
1.2.3. Транспортные карты.....	21
1.2.4. СКУД	22
1.2.5. Телекоммуникации (SIM-карты)	22
1.2.6. Модули безопасности.....	22
1.2.7. Платные информационные услуги	23
1.3. История смарт-карт.....	23
Глава 2. Смарт-карта изнутри	27
2.1. Конструкция смарт-карты.....	27
2.2. Микроконтроллер смарт-карты	29
2.2.1. Структура микроконтроллера для смарт-карты.....	30
2.2.2. Классификация микроконтроллеров для смарт-карт	33
2.2.3. Современные микроконтроллеры для смарт-карт.....	34
2.3. Программное обеспечение смарт-карты.....	36
2.3.1. Системное программное обеспечение	37
2.3.2. Интегрированные приложения	38
2.3.3. Приложения на JavaCard	39
Глава 3. Основные понятия смарт-технологий	41
3.1. Международный стандарт ISO 7816.....	41
3.2. Протокол обмена смарт-карты с внешним миром	42
3.2.1. Логический протокол обмена	42
3.2.2. Формат APDU	44
3.2.3. Заголовок команды	47
3.2.4. Статус завершения команды	48
3.2.5. Контактный интерфейс	51
3.2.6. Радио-интерфейс	52
3.3. Размещение данных на смарт-карте по стандарту ISO 7816.....	53
3.3.1. Приложения для смарт-карт	53
3.3.2. Файловая система.....	54
3.3.3. Свойства файла	56
3.3.4. EF.DIR – каталог приложений.....	56

3.3.5. Жизненный цикл приложения и файла	57
3.4. Типы файлов	59
3.4.1. Приложения и директории.....	59
3.4.2. Бинарные файлы – BF	59
3.4.3. Файлы записей.....	60
3.4.4. Записи в формате TLV	61
3.5. Разграничение доступа к файлам.....	62
3.5.1. Атрибуты доступа к файлу.....	62
3.5.2. Расширенная форма атрибутов доступа	63
3.5.3. Условия доступа	65
3.6. Жизненный цикл смарт-карты	66
3.7. Базовый набор команд согласно стандарту ISO 7816-4.....	67
3.7.1. SELECT APPLICATION.....	67
3.7.2. SELECT FILE	69
3.7.3. ACTIVATE FILE	70
3.7.4. DEACTIVATE FILE	70
3.7.5. READ BINARY.....	71
3.7.6. UPDATE BINARY.....	71
3.7.7. READ RECORD	72
3.7.8. UPDATE RECORD.....	73
3.7.9. APPEND RECORD	73
3.7.10. GET DATA	73
3.7.11. PUT DATA.....	74
3.7.12. CREATE FILE	74
3.7.13. VERIFY	75
3.7.14. CHANGE REFERENCE DATA.....	76
3.7.15. RESET RETRY COUNTER.....	76

Часть II. Основные криптографические алгоритмы и протоколы.....77

Глава 4. Алгоритмы и системы шифрования.....78

4.1. Основные понятия и определения.....	78
4.2. Симметричные алгоритмы.....	83
4.2.1. Стандарты симметричного шифрования DES, Triple DES и AES.....	83
4.2.2. Отечественные стандарты симметричного шифрования	91
4.2.3. Режимы работы алгоритмов блочного шифрования.....	95
4.2.4. Облегченные алгоритмы шифрования.....	102
4.3. Асимметричные алгоритмы.....	107
4.3.1. Асимметричная криптосистема RSA.....	107
4.3.2. Схема Эль-Гамала	111
4.3.3. Асимметричные криптосистемы на базе эллиптических кривых.....	113
4.4. Комбинированные криптосистемы	119

Глава 5. Хеширование и электронная подпись.....122

5.1. Функции хеширования.....	122
5.1.1. Хеш-функции семейства MD.....	123

5.1.2. Алгоритмы семейства SHA.....	126
5.1.3. Отечественные стандарты хеш-функций	137
5.1.4. Коды аутентификации сообщений на основе алгоритмов хеширования.....	141
5.2. Электронные подписи	143
5.2.1. Основные процедуры электронной подписи.....	143
5.2.2. Алгоритм RSA.....	146
5.2.3. Алгоритм DSA.....	147
5.2.4. Алгоритм ECDSA.....	150
5.2.5. Отечественные стандарты электронной подписи	151
5.2.6. Комбинированное применение электронной подписи и шифрования	154
Глава 6. Управление криптоключами	157
6.1. Генерация ключей	157
6.1.1. Генерация случайных чисел.....	157
6.1.2. Обзор статистических тестов.....	162
6.1.3. Генерация случайных простых чисел.....	165
6.1.4. Проверка простоты чисел.....	166
6.2. Использование ключей.....	169
6.2.1. Одноразовые и производные ключи.....	169
6.2.2. Выработка общего ключа шифрования.....	175
6.2.3. Специфика использования ключей в смарт-картах.....	185
6.3. Инфраструктура управления открытыми ключами.....	188
6.3.1. Проблема подмены открытых ключей.....	188
6.3.2. Принципы функционирования инфраструктуры PKI	191
6.3.3. Структура сертификатов открытых ключей.....	195
Глава 7. Методы и протоколы аутентификации.....	202
7.1. Обзор принципов и методов аутентификации.....	202
7.2. Аутентификация с применением сертификатов открытых ключей	208
7.3. Аутентификация на основе симметричных криптоалгоритмов.....	214
7.4. Протокол аутентификации PACE.....	223
7.5. Защищенный обмен сообщениями	235
Часть III. Инфраструктура для работы со смарт-картами.....	237
Глава 8. Спецификации PC/SC.....	238
8.1. Рабочая группа PC/SC и история выпуска спецификаций.....	238
8.1.1. Рабочая группа PC/SC.....	238
8.1.2. Обзор спецификаций PC/SC	240
8.2. Основные требования спецификаций PS/SC.....	244
8.2.1. Требования к интерфейсу совместимых смарт-карт и считывателей.....	244
8.2.2. Требования к интерфейсу считывателей, подключаемых к персональным компьютерам	248
8.2.3. Конструктивные требования к считывателям.....	253
8.2.4. Требования к менеджеру ресурсов смарт-карт	255

8.2.5. Требования к провайдеру сервиса	259
8.2.6. Рекомендации по разработке приложений для смарт-карт.....	264
8.2.7. Рекомендации по применению смарт-карт в приложениях, относящихся к обеспечению безопасности.....	266
8.2.8. Применение считывателей смарт-карт с дополнительными возможностями	270
Глава 9. Управление приложениями согласно спецификации GP	274
9.1. Архитектура карты	275
9.2. Сущности GP	276
9.3. Домены безопасности	277
9.4. Иерархия доменов безопасности.....	279
9.5. Привилегии приложений	280
9.6. Делегированное управление.....	282
9.7. Персонализация	284
9.7.1. Персонализация приложения через домен безопасности (персонализация push-методом)	285
9.7.2. Использование защищенного канала для персонализации приложения (персонализация pull-методом).....	285
9.7.3. Формат данных для персонализации	286
9.8. Управление жизненным циклом	287
9.9. Сервисы	289
9.9.1. Глобальный ПИН.....	289
9.9.2. Сервисы приложений	290
9.10. GP API	290
9.11. Механизмы криптографической защиты информации в GP	290
9.11.1. Защищенный канал	291
9.11.2. Защита исполняемого файла.....	293
9.11.3. Проверочные криптограммы делегированного управления	295
9.12. Пример – муниципальная карта	296
Часть IV. Примеры приложений	299
Глава 10. Домен безопасности GlobalPlatform	300
10.1. Система команд домена безопасности.....	300
10.1.1. SELECT	301
10.1.2. INSTALL	302
10.1.3. LOAD	305
10.1.4. STORE DATA	306
10.1.5. PUT KEY.....	306
10.1.6. SET STATUS	308
10.1.7. DELETE.....	309
10.1.8. GET DATA.....	310
10.1.9. GET STATUS.....	311

10.2. Защищенный канал обмена	311
10.2.1. Уровни безопасности	311
10.2.2. Опции протокола SCP-02	312
10.2.3. Установка защищенной сессии	314
10.2.4. Защищенный обмен сообщениями	319
10.3. Типичные сценарии использования GP	321
10.3.1. Загрузка и установка приложения	322
10.3.2. Персонализация приложения push-методом	324
10.3.3. Персонализация приложения pull-методом	324
10.3.4. Блокирование и разблокирование приложения	325
10.3.5. Удаление приложения	325
Глава 11. Криптографический токен	327
11.1. Защита информации в криптографическом токене	327
11.2. Система команд ISO 7816 для криптографического токена	330
11.3. Управление ключами	331
11.3.1. GENERATE ASYMMETRIC KEY PAIR	332
11.4. Настройка среды безопасности	333
11.5. Криптографические операции	335
11.5.1. Шифрование данных	335
11.5.2. Расшифровка данных	336
11.5.3. Вычисление криптографической контрольной суммы	336
11.5.4. Проверка криптографической контрольной суммы	337
11.5.5. Вычисление хеша	337
11.5.6. Вычисление электронной подписи	337
11.5.7. Проверка электронной подписи	338
11.5.8. Проверка сертификата	338
11.6. Криптографическое приложение	339
11.6.1. Файловая система криптографического приложения	340
11.6.2. Содержание файлов криптографического приложения	342
11.7. Пример криптографического приложения	345
11.7.1. Файловая структура токена	345
11.7.2. Сценарий генерации ЭП при помощи токена	347
Глава 12. Электронное удостоверение личности	349
12.1. Международные паспортно-визовые документы	351
12.2. Структура данных международного паспорта	353
12.3. Механизмы аутентификации в международном паспорте	356
12.3.1. Пассивная аутентификация	357
12.3.2. Аутентификация на основе MRZ	358
12.3.3. Расширенный контроль доступа и активная аутентификация	363
12.4. Управление доступом и PKI	369
12.4.1. Условия доступа	369
12.4.2. Инфраструктура выпуска ЭД	369
12.4.3. Инфраструктура приема ЭД	370

12.4.4. CV-сертификаты	371
12.5. Защищенный обмен сообщениями в международном паспорте	372
12.6. Система команд международного паспорта	377
12.6.1. GET CHALLENGE	377
12.6.2. MUTUAL AUTHENTICATE (BAC)	377
12.6.3. MSE: SET AT (PACE)	378
12.6.4. GENERAL AUTHENTICATE	378
12.6.5. MSE: SET KAT (Аутентификация микросхемы)	379
12.6.6. MSE: SET AT (Аутентификация терминала)	380
12.6.7. PSO: Verify Certificate	380
12.6.8. EXTERNAL AUTHENTICATE (Аутентификация терминала)	381
12.6.9. INTERNAL AUTHENTICATE	381
12.7. Сценарий чтения паспорта	381
12.7.1. Выбор приложения и установка ЗОС на основе MRZ	382
12.7.2. Пассивная аутентификация	383
12.7.3. Активная аутентификация	383
12.7.4. Расширенный контроль доступа (EAC)	384
12.7.5. Чтение данных	384
Глава 13. Платежная карта EMV	385
13.1. Назначение платежной карты	385
13.2. Приложение EMV	388
13.2.1. Данные EMV-приложения	388
13.2.2. EMV-транзакция	388
13.2.3. Система команд приложения EMV	392
13.2.4. Пример транзакции	393
13.3. Информационная безопасность в приложении EMV	395
13.3.1. Аутентификация карты	395
13.3.2. Шифрование ПИН-кода	396
13.3.3. Криптограмма приложения и криптограмма эмитента	396
13.3.4. Скрипты эмитента	396
13.3.5. Российская криптография для платежного приложения	397
13.4. Неплатежные применения банковских карт	397
13.4.1. СКУД	399
13.4.2. Аутентификация в системе ДБО	399
13.4.3. Транспортная карта	399
13.5. Российская платежная карта МИР	400
13.6. Спецификация EMV нового поколения	402
Часть V. Технология JavaCard	403
Глава 14. Знакомство с JavaCard	404
14.1. Отличия JavaCard от Java	405
14.1.1. Язык программирования JavaCard	405
14.1.2. Виртуальная машина JavaCard	406

14.1.3. Среда исполнения	407
14.1.4. Стандартный API.....	407
14.2. Знакомство с апплетами	408
14.2.1. Основные сущности JavaCard	408
14.2.2. JavaCard Framework	409
14.2.3. Создание и регистрация апплета.....	410
14.2.4. Диспетчер команд.....	411
14.2.5. Обработчик команды	412
14.3. Подготовка апплетов.....	413
14.3.1. Сборка апплета.....	413
14.3.2. Установка апплета	413
14.4. Данные в JavaCard	414
14.4.1. Объекты	415
14.4.2. Транзиентные массивы.....	415
14.4.3. Глобальный массив	417
14.4.4. Атомарность операций	417
14.5. Исключения.....	419
14.6. Изоляция апплетов.....	422
14.6.1. Обзор	422
14.6.2. Разделяемые объекты.....	424
Глава 15. JavaCard API	426
15.1. Главное – пакет javacard.framework.....	427
15.1.1. Класс Applet.....	428
15.1.2. Класс JCSysyem.....	429
15.1.3. Ввод/вывод	430
15.1.4. Исключения.....	433
15.2. Криптография в JavaCard.....	433
15.2.1. Структура криптографической библиотеки	433
15.2.2. Ключи.....	434
15.2.3. Криптографические алгоритмы.....	436
15.2.4. Российская криптография.....	438
15.3. Полезные классы и утилиты.....	439
15.3.1. Утилиты	439
15.3.2. Поддержка ПИН'а.....	440
15.3.3. Дополнительные расширения JC API в картах Микрона	441
15.4. Global Platform API.....	441
15.4.1. Обзор Global Platform API.....	441
15.4.2. Класс GPSystem	442
15.4.3. Средства GP API для персонализации апплетов.....	443
Глава 16. Примеры апплетов на JavaCard.....	445
16.1. Средства разработки	445
16.1.1. Подготовка инфраструктуры.....	445
16.1.2. Сборка апплета вручную	445

16.1.3. Скрипт сборки	446
16.2. Простейший апплет	447
16.3. Hello, JC!	448
16.4. Криптографическое приложение	455
16.4.1. Спецификация приложения	455
16.4.2. Команды приложения	457
16.4.3. Исходный код апплета	458
16.5. Советы программистам на JavaCard	470
16.5.1. Объекты	470
16.5.2. Транзистентная память	470
16.5.3. Буферы	470
16.5.4. Транзакции	471
16.5.5. Арифметические операции в JC	471
16.5.6. Методы в JavaCard	472
16.5.7. Исключения	472
16.5.8. Особенности реализации	473
Заключение	474
Приложение А. Web-сайт книги	475
Приложение Б. Утилита Smacon	476
Приложение В. Формат TLV	480
Приложение Г. Таблицы стандарта шифрования ГОСТ Р 34.12-2015	482
Приложение Д. Таблицы стандарта хеширования ГОСТ Р 34.11-2012	485
Англо-русский словарь терминов	489
Список сокращений	491
Перечень источников	498

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)	Закрит
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-

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru