

УДК 004.03
ББК 32.972
М94

М94 Мытник К. Я., Панасенко С. П.

Смарт-карты и информационная безопасность / под редакцией д. т. н., профессора В. Ф. Шаньгина – М.: ДМК Пресс, 2019. – 516 с.: ил.

ISBN 978-5-97060-690-2

Книга предназначена для специалистов в области информационных технологий, связанных с использованием смарт-карт. Она освещает такие сферы применения смарт-карт как платежные системы, электронные документы, системы управления доступом и некоторые другие. Книга может быть полезна студентам, аспирантам и научным работникам, интересующимся смарт-картами.

УДК 004.03
ББК 32.972

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-97060-690-2 (рус.)

© Мытник К. Я., Панасенко С. П., 2018
© Оформление, издание, ДМК Пресс, 2019

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 JCSystem.....	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. Транзиентная 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