

УДК 336.717+004
ББК 65.262.32+32.973.26-018.2
Г60

Руководитель проекта, выпускающий редактор
А.С. Воронин

Голдовский И.

Г60 Банковские микропроцессорные карты / И.М. Голдовский — М.:
ЦИПСИР: Альпина Паблишерз, 2010. — 686 с.

ISBN 978-5-9614-1233-8

Книга дает читателю систематизированное представление о современных микропроцессорных картах, используемых в банковском деле. Она может служить путеводителем по объемным книгам, содержащим описание стандарта EMV, и спецификациям приложений ведущих платежных систем. Книга содержит системное описание стандарта EMV, делая акцент на разъяснение наиболее важных аспектов, тонкостей и особенностей реализации лежащих в его основе методов и алгоритмов. Подробно анализируется эффект от внедрения технологии микропроцессорных карт на безопасность карточных операций. Исследуется влияние внедрения микропроцессорных карт на процессинговую систему банка, предлагаются рекомендации по технологии выбора решений для миграции банка на микропроцессорные карты. В книге значительное внимание уделено открытым операционным системам, используемым в микропроцессорных картах, а также универсальной платформе GlobalPlatform, находящей все большее применение для безопасной удаленной загрузки, инсталляции, экстракции приложений и их конфигурирования после выпуска карты. Отдельная глава посвящена бесконтактным банковским платежам, а также мобильным платежам.

УДК 336.717+004
ББК 65.262.32+32.973.26-018.2

Все права защищены. Никакая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, включая размещение в сети Интернет и в корпоративных сетях, а также запись в память ЭВМ для частного или публичного использования, без письменного разрешения владельца авторских прав. По вопросу организации доступа к электронной библиотеке издательства обращайтесь по адресу lib@alpinabook.ru.

© И.М. Голдовский, 2010
© ООО «Центр исследований
платежных систем и расчетов», 2010
© ООО «Альпина Паблишерз», 2010

ISBN 978-5-9614-1233-8

ОГЛАВЛЕНИЕ

Принятые сокращения	7
----------------------------------	---

Введение	9
-----------------------	---

Глава 1

ОСНОВНЫЕ СВЕДЕНИЯ О ПЛАСТИКОВЫХ КАРТАХ	15
---	----

1.1. Основные понятия и определения	15
1.2. Стандарты в области карт с магнитной полосой	26
1.3. Содержание дорожек магнитной полосы карты	31
1.4. Межхостовой интерфейс	35
1.5. Проблема безопасности карточных операций	40
1.6. О стандартах для микропроцессорных карт	76

Глава 2

ОБЩИЕ СВЕДЕНИЯ О МИКРОПРОЦЕССОРНЫХ КАРТАХ	93
--	----

2.1. Общие характеристики смарт-карт	93
2.2. Архитектура микросхемы	100
2.3. Начальная установка карты	114
2.4. Коммуникационные протоколы	126
2.5. Производство микропроцессорных карт	140
2.6. Многоприкладные операционные системы	145
2.7. Платформа GlobalPlatform	154
2.8. Оценка физической безопасности микропроцессорной карты	166
2.9. Общие тенденции развития микропроцессорных карт	182

Глава 3

ФАЙЛОВАЯ СТРУКТУРА,

КОМАНДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ДАННЫХ

В МИКРОПРОЦЕССОРНЫХ КАРТАХ СТАНДАРТА EMV	185
---	-----

3.1. Объекты данных и их кодировка	185
3.2. Общие сведения о файловой структуре карты	189

4 БАНКОВСКИЕ МИКРОПРОЦЕССОРНЫЕ КАРТЫ

3.3. DF-файлы	192
3.4. EF-файлы	195
3.5. ADF-файлы	198
3.6. AEF-файлы	204
3.7. DDF-файлы	205
3.8. PSE-файл	207
3.9. Команды	208
3.10. Примеры команд	213
3.11. Вопросы безопасности в стандарте EMV	226
3.12. Методы офлайновой аутентификации карты	236
3.13. Шифрование PIN-кода при его проверке в офлайновом режиме	255
3.14. Прикладная криптограмма (Application Cryptogram) и аутентификация эмитента	259
3.15. Защищенная передача данных (Secure Messaging)	262
3.16. Управление ключами	264

Глава 4

ОБРАБОТКА ТРАНЗАКЦИИ ПО МИКРОПРОЦЕССОРНОЙ КАРТЕ

4.1. Выбор технологии	278
4.2. Выбор приложения	282
4.3. Инициализация транзакции	289
4.4. Чтение данных карты	295
4.5. Аутентификация карты	300
4.6. Проверка ограничений на обработку транзакции (Processing restrictions)	306
4.7. Верификация держателя карты	310
4.8. Процедуры управления рисками, выполняемые терминалом (Terminal Risk Management)	322
4.9. Оценка результатов выполненных терминалом процедур (Terminal Action Analysis)	327
4.10. Процедуры управления рисками, выполняемые картой (Card Risk Management)	340
4.11. Процесс принятия решения картой (Card Action Analysis)	355



4.12. Онлайн-обработка транзакции и аутентификация эмитента	366
4.13. Процедура Issuer Script Processing.	371

Глава 5

ПЕРСОНАЛИЗАЦИЯ КАРТ	377
----------------------------------	-----

5.1. Жизненный цикл карты	377
5.2. Персонализация карт	380

Глава 6

ОСОБЕННОСТИ МИГРАЦИИ НА МИКРОПРОЦЕССОРНЫЕ КАРТЫ	395
--	-----

6.1. Постановка задачи миграции на МПК.	395
6.2. О выборе метода аутентификации карты	426
6.3. О методе верификации держателя карты	439
6.4. О выборе терминала	442
6.5. Совместимость приложений терминала и карты	445
6.6. Анализ реальной безопасности операций по МПК	451
6.7. Управление ключами	484
6.8. Выбор аппаратно-программной платформы МПК и конфигурации ее приложения	487
6.9. Влияние миграции на систему эмитента	491
6.10. Влияние миграции на систему обслуживающего банка	501

Глава 7

БЕСКОНТАКТНЫЕ КАРТЫ	503
----------------------------------	-----

7.1. Причины интереса к бесконтактным картам	504
7.2. Основы технологии	508
7.3. Используемые стандарты	512
7.4. Протоколы взаимодействия карты и терминала прикладного уровня	522
7.5. MasterCard PayPass	525
7.6. VISA Contactless	530
7.7. Стандарт Entry Point Specification	539
7.8. Протокол NFC и его использование в сотовых телефонах. . .	546
7.9. Вопросы безопасности бесконтактных платежей	562

6 БАНКОВСКИЕ МИКРОПРОЦЕССОРНЫЕ КАРТЫ

Глава 8

СРАВНЕНИЕ EMV-СОВМЕСТИМЫХ ПРИЛОЖЕНИЙ575

- 8.1. Объекты данных и команды577
- 8.2. Сравнение функциональности приложений.....586
- 8.3. Безопасность операций.....612
- 8.4. Оценка сложности имплементации приложений615

Заключение621

Приложение А

Математические основы криптографии627

Приложение В

Введение в криптографию643

MasterCard® PayPass™677

«Жемальто» — мировой лидер в области технологий цифровой безопасности681

Список рекомендуемой литературы683