УДК 621.794.61:621.357.8:669.71

ОСОБЕННОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ В США И ЕВРОПЕ

Ю.В. БОРОДАЕНКО

Маунтэн-Вью, Калифорния, 94040, Соединенные Штаты Америки
daenko@gmail.com

Рассматриваются элементы и отличия электронных платежей в США и Европе. Приведены процесс защиты, обработка смарт-карт, инфраструктура, технология авторизации, обработка транзакций и перспективы развития.

Ключевые слова: электронный платеж, смарт-карты, EMV, технология авторизации.

В 1993 г. ведущие платежные системы Europay, MasterCard, и Visa (EMV) подписали соглашение об использовании смарт-чипов при оплате счетов кредитными и дебетовыми картами под названием EMV. По данным ассоциации EMV, смарт-карты составляют лишь около 40 % в мировом обороте банковского «пластика», и подавляющее большинство пластиковых карт в США – это карты с магнитной полосой [1]. При платеже ее проводят через считывающее устройство, после чего держатель пластиковой карты должен подписать квитанцию по транзакции; вводить PIN-код не требуется. Европа начала переход на карты EMV (чип + PIN) в 2004 году потому, что эти карты являются более эффективными в предотвращении мошенничества. Почему в США преобладают магнитные карты и является ли этот способ платежей менее защищенным и безопасным – рассмотрено в докладе.

Процесс защиты. Процесс защиты смарт-карты является многоступенчатым, первая ступень – встроенный уникальный код, который индивидуален для каждой микросхемы. Вторая ступень защиты устанавливается при выдаче карточки пользователю, в базу данных заносится несколько секретных PIN-кодов, которые известны только владельцу карты. Кроме того, чип, помещенный внутри карты, повредить намного сложнее, чем магнитную полосу, которую можно поцарапать или размагнитить. Таким образом, переход на технологию EMV был обусловлен борьбой с кредитно-карточным мошенничеством, когда воры копируют данные карт с магнитной полосой. А размах кредитно-карточного мошенничества в США впечатляет: в конце 2013 г. во время предновогодних распродаж была реализована атака на одну из крупнейших розничных сетей Target, в результате за 19 дней были похищены данные о 70 млн платежных карт пользователей.

Обработка карты и инфраструктура. Известно, что смарт-карты обрабатываются с помощью считывающих устройств, отличающихся от тех, которые используются для карт с магнитной полосой. Нежелание переходить на карты чип+PIN может создать впечатление, что США отстают в технологии кредитных карт, но это не так просто. Одной из причин задержки, как сообщает источник [2], является то, что в США эмитенты отделены от системы обработки платежей, и не в состоянии заставить торговцев покупать новые терминалы, необходимые для обработки карт чип + PIN.

В Европе эмитенты карт имеют больше контроля над инфраструктурой процессинга карт торговцев. «Наша платежная система имеет слишком много уровней и является очень сложной», – говорит Рэнди Вандерхуф (Randy Vanderhoof), исполнительный директор Альянса Смарт-Карт (Smart Card Alliance) [2].

Технология авторизации. Следующей особенностью электронной платежной системы в США является то, что система проверки кредитных карточек работает в режиме on-line, в отличие от проверки смарт-карт в режиме off-line. Все объясняется осо-

бенностями телефонной связи: в точке продажи продавец использует модем, чтобы убедиться в том, что карточка действительна и клиент платежеспособен. Двадцать лет назад эта система не могла бы работать ни в одной европейской стране, плата за телефон была высока, связь была дорогой и ненадежной. Создание онлайновой системы в Европе было невыгодно, поэтому индустрия отдала предпочтение смарт-картам, позволявшим хоть как-то обезопасить сделки – для работы со смарт-картой не нужен постоянный доступ к центрам авторизации, ее можно осуществлять в режиме off-line, что экономит средства и время на доступ к связному оборудованию. [2]

Обработка транзакций. При осуществлении on-line авторизации техническое взаимодействие с точками обслуживания осуществляют процессинговые центры. Банки-эквайеры осуществляют лишь функции расчетов с обслуживающими карточками предприятиями и авторизуют транзакции on-line банков при технических сбоях. Для систем с off-line авторизацией проблема маршрутизации транзакций имеет меньшее значение, поскольку авторизация в таких системах происходит непосредственно в точке обслуживания. Пересылка же транзакций для обеспечения проведения взаиморасчетов происходит не в режиме реального времени. Кроме того, формирование итоговых данных для проведения взаиморасчетов происходит в одном или нескольких процессинговых центрах, что также уменьшает требования к коммуникационным возможностям системы. Таким образом, переход на систему EMV – это не просто замена оборудования в торговых точках, требующая многомиллиардных инвестиций, а это серьезные изменения в бизнес-процессе платежа, требующие кроме инвестиций принятия ряда законодательных и юридических решений.

Перспективы. Компании США активно противятся внедрению смарт-карт, считают, что прогресс должен состоять в переходе на бесконтактные карты без полосы. Банки поддерживают переход на EMV в качестве способа борьбы с кредитно-карточным мошенничеством, когда хакеры копируют данные карт с магнитной полосой. В то время как EMV давно применяется в Европе и Канаде, американские продавцы отказывались тратиться на модернизацию. В то же время Visa намеревается увеличить объем продаж новых терминалов и ускорить переход на транзакции, производимые с помощью мобильных телефонов с NFC-чипами. По данным исследования Crone Consulting LLC, всего 200 тыс. из 6 млн. магазинных терминалов могут принимать бесконтактные платежи. Старший аналитик Aite Group LLC считает, что этот шаг Visa ускорит распространение мобильных платежей на год. К 2015 г. общий мировой объем таких платежей за цифровые и физические товары, денежных переводов и NFC-транзакций достигнет 670 млрд долл. США, тогда как в 2011 г., по данным Juniper Research, он составил всего 240 млрд долл. Согласно информации Smart Card Alliance, сертификация систем безопасности Visa ежегодно обходится предприятиям более чем в 2 млрд долл. [3]

Список литературы

1. Сравниваем смарт-карты и магнитные пластиковые карты. – [Электронный ресурс], – Режим доступа: http://smartcardinfo.com/basics/4-2011-09-08-13-41-07.html. – Дата доступа: 10.01.2014.

2. *Варфоломеев А.А.* Защита информации с использованием интеллектуальных карт. – [Электронный ресурс], – Режим доступа: web-local.rudn.ru/web-local/uem/iop_pdf/53-varfolomeev.pdf. – Дата доступа: 10.01.2014.

3. The US Adoption of Computer-Chip Payment Cards. – [Электронный ресурс], – Режим доступа: www.kc.frb.org/publicat/econrev/pdf/13q1Sullivan.pdf. – Дата доступа: 10.01.2014.