

Смарт-карты известны участникам российского рынка еще с первой половины 1990-х годов. Именно тогда на их базе был создан целый ряд локальных и межрегиональных систем. Побудительными мотивами при создании таких систем в то время служили, в том числе, и финансово-организационные сложности при вступлении банков в международные платежные системы, и неразвитость телекоммуникаций, что вызывало необходимость обслуживать карты в режиме offline. Поэтому эмитентами в рамках таких систем выступали не только финансовые учреждения, но и крупные предприятия, властные структуры регионального уровня и т. д. Данные системы были построены на закрытых спецификациях системных интеграторов, использовали ограниченное число типов терминальных устройств (POS-терминалов, банкоматов), но в то же время были ориентированы на реальные потребности заказчиков. Некоторые из этих систем дожили до сегодняшнего дня, и только крупнейшие из них – «СБЕРКАРТ» и «Золотая Корона» – насчитывают в своем портфеле по несколько миллионов реально обращающихся карт. Кроме банковского сектора, такие системы с успехом работают в сегменте топливных компаний, обслуживаясь в сетях АЗС и обеспечивая оплату ГСМ и сопутствующих товаров.

Основными недостатками таких систем являлась и является закрытость спецификаций и, как следствие, большие сложности в решении вопросов развития системы, обеспечения широкого приема ее карт в масштабах всей территории страны. В те же 1990-е международные платежные системы, использовавшие тогда традиционные магнитные карты, столкнулись с ростом карточного мошенничества, обусловленного сравнительной простотой подделки платежных карт, а также с необходимостью сделать свои карточные продукты более привлекательными для конечного потребителя за счет предоставления ему с их помощью допол-

Выбор типа EMV-карты: от бизнес-требований до сертификации в платежной системе

Вадим Кохно, главный специалист ЗАО «ПРОНИТ», группа компаний КАРТХОЛЛ
Юрий Перлин, зам. генерального директора ЗАО «ПРОНИТ», группа компаний КАРТХОЛЛ



Вадим Кохно

нительных услуг помимо традиционной платежной функции. Так возникли спецификации EMV (Europay, MasterCard, Visa), позволившие обеспечить прием смарт-карт по всему миру.

Реальная эмиссия карт с EMV-приложениями началась в России и странах СНГ в 2002–2003 годах.

Первая волна этого процесса пришлась на 2005–2007 гг. и была связана с переносом ответственности, введенным международными платежными системами. К настоящему моменту практически все крупнейшие отечественные эмитенты карт Visa и MasterCard с успехом завершили процесс сертификации обслуживания и эмиссии EMV-карт. Однако следует отметить, что среди этих банков только еди-



Юрий Перлин

ницы действительно обеспечили реальную миграцию с карт с магнитной полосой на смарт-карты, полностью или почти полностью перейдя на выпуск только карт, соответствующих спецификациям EMV.

В настоящее время процесс миграции эмитентов на EMV обретает на отечественном рынке второе дыхание благодаря тому, что одни банки приступают к массовой эмиссии EMV-карт, а другие расширяют номенклатуру выпускаемых карточных продуктов на микропроцессорной платформе. Несомненно, что «вторая волна» EMV-эмиссии будет более пологой и растянутой во времени, но в то же время и более масштабной – не только с точки зрения абсолютного количества выпущенных EMV-карт, но и в отношении их

доли в общей карточной эмиссии. Уже сейчас в Москве и других крупных городах чиповые операции в POS-терминалах составляют значительную часть от общего числа карточных транзакций.

Различные производители карт, в том числе такие известные, как Gemalto, Giesecke & Devrient, Oberthur, Sagem Orga, предлагают достаточно большое количество сертифицированных карточных продуктов, удовлетворяющих спецификациям Visa VSDC и MasterCard M/Chip. Кроме того, на рынке постоянно появляются все новые и новые типы карт. В связи с этим нам представляется весьма своевременным обсудить принципы оптимального выбора типа EMV-карт, удовлетворяющего всем современным требованиям банка-эмитента.

Определение терминологии и классификации

Несомненно, что главенствующим фактором при выборе того или иного типа EMV-карты должно быть соответствие данного карточного продукта бизнес-задачам, решаемым банком-эмитентом. Объем памяти, производительность процессора, скорость обмена информацией с терминальным устройством и прочие технические характеристики карты являются вторичными параметрами, призванными обеспечить ее необходимую функциональность. В качестве примера, подтверждающего первичность бизнес-задач по сравнению с техническими характеристиками карты, можно привести методологию классификации карт, которую приняла компания Gemalto, проводя ребрен-

динг своих продуктовых линеек после слияния Gemplus и Axalto. Если раньше карты в первую очередь классифицировались по типу используемой операционной системы (Java Card или native) и названия продуктам давались в соответствии с названием ОС, то теперь название карты сначала определяет ее функциональные возможности, а уже затем параметрически описывает, за счет чего эти возможности удовлетворяются.

Тем не менее, для того чтобы в дальнейшем можно было привести в соответствие технические характеристики карт решаемым с их помощью бизнес-задачам, необходимо осуществить общую классификацию применяемых в настоящее время EMV-карт.

EMV-карты можно разделить на два больших класса по типу используемой операционной системы:

- с открытыми операционными системами (Java Card, Multos);
- с операционной средой, разработанной производителем для конкретного продукта – native (или proprietary) карты.

Лет пять-семь назад к картам с открытой операционной системой относили также и Windows for Smart Card (WfSC), однако сейчас последние можно считать закрытым проектом, не получившим поддержки производителей карт.

Карты с ОС Multos не получили распространения в России и странах СНГ из-за сложности административных процедур получения разрешения на их выпуск и организационно-сложной технологии формирования криптографических данных.

В свою очередь, в зависимости от наличия или отсутствия крипто-сопроцессора, обеспечивающего несимметричную RSA криптографию, карты подразделяются на:

- карты со статической аутентификацией (SDA);
- карты с динамической и/или комбинированной аутентификацией (DDA/CDA), которые, как правило, также поддерживают проверку на карте шифрованного ПИН-кода.

КАЛЕЙДОСКОП

Решение Diasoft FA# Retail внедрено в ЭКСПОБАНКе

Компания «Диасофт» завершила работу по внедрению решения для автоматизации розничной деятельности Diasoft FA# Retail в ЭКСПОБАНКе. В частности, с использованием решения были автоматизированы процессы таких видов кредитования, как потребительское, ипотечное и автокредитование.

При установке продукта в банке была использована технология «Типового внедрения», включающая поставку комплекта дистрибутивного банковского функционала, в том числе настроенных типовых банковских продуктов, а также инструментарий с описанием механизмов документооборота и бизнес-процессов.

Сотрудничество «Диасофт» и ЭКСПОБАНК началось в 1999 г. В настоящее время, помимо автоматизированной системы кредитования физических лиц, в банке установлены решения

для корпоративного обслуживания Diasoft FA# Bank, продукты для поддержки работы на финансовых рынках Diasoft FA# Treasury и автоматизации процессов внутрихозяйственной деятельности Diasoft FA# Balance.

Райффайзен Банк Аваль: денежные переводы за 1 гривну

С 1 апреля по 30 июня 2008 г. Райффайзен Банк Аваль (г. Киев, Украина) проводит акцию для держателей карточек Visa Int. и MasterCard Worldwide, обслуживающихся в рамках тарифного плана «Оптимальный». Комиссия за перевод средств (в гривнах) в рамках сервиса «АТМ-Экспресс» по всей территории Украины для держателей данных карт составит 1 гривну (0,2 долл. США) вне зависимости от суммы перевода.

Сумма денежного перевода не должна превышать 80 тыс. гривен (15 тыс. долл. США). Размер комиссии за перевод для держателей карт, обслуживающихся в рамках других тарифных планов, составляет 1% от суммы перевода. ▲

Еще 5 лет назад задача размещения в смарт-карте RSA-сопроцессора представлялась довольно сложной. Сегодня все производители смарт-карт имеют в своих линейках продукты карты с крипто-сопроцессором, тем не менее цена таких карт все еще несколько выше, чем карт без сопроцессора.

Де-факто EMV-карты международных платежных систем могут работать через контактный и/или бесконтактный интерфейс. В зависимости от поддерживаемого картой интерфейса к обслуживающим устройствам (устройствам чтения/записи) карты можно подразделять на четыре типа:

- контактные карты;
- бесконтактные карты;
- комбинированные карты (два интерфейса к одному чипу);
- гибридные карты (карты с двумя чипами – с контактным и бесконтактным интерфейсами).

Строго говоря, бесконтактные карты не являются самостоятельным типом EMV-карт, поскольку спецификации EMVCo описывают только транспортный уровень взаимодействия с бесконтактной картой. Реализации же бесконтактных финансовых приложений у Visa и MasterCard в настоящий момент имеют целый ряд принципиальных различий.

Несмотря на то что EMVCo (а также Visa) специфицировали общие правила персонализации карт с EMV-приложениями, не все карты соответствуют спецификациям Card Personalization Specification (CPS). Подавляющее большинство native карт этим спецификациям не удовлетворяют.

В связи с этим EMV-карты можно подразделять на:

- карты и приложения, поддерживающие CPS;
- карты и приложения, для которых требуется специфическая программа персонализации.

В зависимости от возможности загрузки на карту приложений после ее изготов-

ления карты можно разделить на следующие классы:

- «статические» карты (native и Java Card «S»);
- «динамические» карты (полнофункциональные Java Card и карты Multos).

«Статические» карты могут использовать лишь приложения, размещенные на карте в процессе ее производства. «Динамические» карты предоставляют возможность загрузки произвольных приложений в процессе эмиссии карт (в допол-

нение к приложениям, размещенным на карте в процессе ее производства).

Итак, мы ввели некоторый набор классификаций EMV-карт, чтобы в дальнейшем, в зависимости от решаемых эмитентом задач, можно было четко определить, к какому типу в рамках каждой классификации относится требуемая ему карта, последовательно используя метод «исключения» типов карт, не соответствующих бизнес-требованиям банка.

Цели EMV-миграции

Прежде чем приступать к выбору EMV-карты, необходимо четко определить все бизнес-цели, которых банк стремится достичь с помощью ее эмиссии. Иными словами, необходимо четко сформулировать, зачем эмитенту нужна EMV-миграция.

Некоторые банки бывают в этом случае настроены «попробовать воду»: пройти сертификацию в платежной системе, получить начальный опыт в работе с чиповыми картами, минимизируя при этом затраты на реализацию первой стадии EMV-миграции. Массовая эмиссия откладывается на обозримый, но не вполне определенный срок. В этом случае можно рекомендовать для тестирования самую простую и, соответственно, бюджетную карту. Если же банк уже четко определил стратегические цели развития своей EMV-программы в долгосрочной перспективе, и, соответственно, сформулировал конкретные требования к карточному продукту, ему следует обратить внимание на карту, полностью удовлетворяющую данным требованиям.

Следует отдавать себе отчет, что иногда единственным результатом данного мероприятия будет практический опыт сотрудников банка по эмиссии EMV-карт. С определенной степенью вероятности к тому времени, когда в банке приступят к массовой эмиссии EMV-карт, тот тип карточного продукта, с которым эмитент проходил сертификацию, будет снят с производства.

В таком случае сертификацию необходимо будет проходить в платежной системе повторно, потребуется модернизация персонализационного решения (более простая, зачастую сводящаяся к дополнительным настройкам системы, в случае с картами, поддерживающими CPS, несколько более сложная в случае с native картами).

В случае планирования массового выпуска EMV-карт прежде всего необходимо обсудить следующие функциональные возможности карты:

- Должна ли карта поддерживать работу в режиме offline, а также предавторизованный дебет? Платежные системы настоятельно рекомендуют для карт с такой функциональностью реализацию аутентификации динамических данных (DDA/CDA);

- Планирует ли банк предоставлять клиентам услугу home banking и аналогичную ей, с использованием на карте технологии генерации одноразовых паролей CAP/DPA? В случае положительного ответа необходимо выставить требование поддержки приложения CAP/DPA на карте.
- В случае эмиссии карт, содержащих дополнительные приложения стандарта, отличного от EMV, например:
 - лояльности;
 - топливное приложение;
 - приложение типа «электронный кошелек»;
 - социальные приложения;
 - транспортное приложение,
 следует удостовериться, что технологические особенности выбираемой карты позволят разместить на ней требуемые приложения и обеспечить их совместную работу.
- Если часть приложений планируется размещать или персонализировать после выдачи карты ее владельцу, то карта должна поддерживать режим постэмиссии приложений и обладать достаточным для размещения новых приложений объемом памяти;
- Обслуживание карт через бесконтактный интерфейс по технологии MasterCard PayPass или Visa payWave. Карты, поддерживающие бесконтактный интерфейс, превосходят по цене контактные карты, и прежде чем принимать решение о выборе карты с контактно/бесконтактным интерфейсом, необходимо четко определить область применения бесконтактного интерфейса.

Возможности карты и функционирование EMV-приложения

В технической документации на карту с EMV-приложением всегда указываются спецификации EMVCo и платежной системы, которым соответствует финансовое приложение карты. Однако это не обеспечивает поддержку всех описанных в спецификации функциональных возможностей, а лишь гарантирует отсутствие противоречий между приложением и указан-

ной спецификацией. Как правило, документация поставщика содержит достаточную информацию о функциональных возможностях карты и EMV-приложения на ней, но иногда обнаруживаются и недокументированные «свойства» продукта, поэтому единственным критерием истины остается практика: только после проверки работоспособности тестовой карты во всех требуемых режимах можно быть уверенным, что карта действительно отвечает предъявленным требованиям.

При миграции с одного типа карты на другой, с аналогичной функциональностью, зачастую могут также потребоваться изменения в списке персонализируемых данных. Иными словами, набор параметров, необходимый для реализации одной и той же функциональности, может зависеть от типа карты. Допустим, банк мигрирует с Java-карты с апплетом поставщика карт, соответствующим спецификации VSDC 1.4.0 и поддерживающим:

- аутентификацию данных в режиме DDA/CDA;
- протоколирование транзакций в карте;
- передачу значений offline-счетчиков на хост эмитента, на карту с апплетом Visa v.2.5.1 (последний реализует аналогичную функциональность). При этом апплет Visa поддерживает 4-байтную длину ADA, а «старая» карта поддерживала 2-байтную длину, т. к. типы транзакций (offline/online/decline), протоколируемые апплетом, апплетом не настраивались. Аналогичным образом могут отличаться и значения других параметров карты.

С другой стороны, время от времени банкам предлагают EMV-карты «точно такие же, как у производителя N, но на 30% дешевле». При тестировании действительно может оказаться, что представленная карта в точности повторяет всю функциональность карты производителя N. Однако если эта карта не включена в список карточных продуктов, одобренных платежной системой (Approval ID), то, вероятнее всего, пройти сертификацию в платежной системе с такой картой банку не

удастся. Рекомендуется также проверить дату возобновления (Renewal Date) одобрения карты платежной системой. Если платежная система не продлит срок возобновления после его истечения, то, скорее всего, производитель в скором времени прекратит выпуск данных карт как устаревших, и банку придется мигрировать на другой тип карты. В платежной системе Visa список одобренных продуктов находится в открытом доступе на сайте partnernetwork.visa.com, в свою очередь, MasterCard предоставляет эту информацию банкам по запросу.

Конечно, возможные рекомендации по анализу даты возобновления одобрения карты платежной системой сложно сформулировать абсолютно четко: в случае неопределенности перспектив продления сроков одобрения карты в платежной системе в этом вопросе могут помочь либо специалисты технической поддержки платежной системы, либо собственное объективное представление банка о том, насколько функциональные возможности карты удовлетворяют современным требованиям платежной системы и бюллетеням EMVCo.

Резюмируя вышесказанное, можно отметить, что при выборе типа карты с EMV-приложением следует учитывать:

- возможности карты и EMV-приложения, размещенного на ней (ограничения, накладываемые производителем карт);
- требования эмитента к функциональным возможностям карты и ее приложений – как финансовым (online/offline, контроль международных и иновалютных операций по карте, географические ограничения обслуживания карты), так и дополнительным (loyalty, топливным и т. д.);
- требования платежной системы (наличие Approval ID карты с конкретным приложением и актуальная Renewal Date).

Подходы к выбору карты

Критериями выбора карты являются:

- функциональные возможности EMV-приложения;

- номенклатура дополнительных приложений на карте;
- стоимость EMV-проекта (эмиссии и обслуживания).

Решая задачу минимизации стоимости EMV-решения при условии выполнения сформулированных бизнес-требований и учетом дальнейшего развития системы, нельзя ограничиваться только оценкой стоимости самих карт. Стоимость EMV-решения включает в себя следующие основные составляющие:

- стоимость EMV-карты;
- стоимость сертификации карты в платежной системе;
- стоимость персонализационного решения;
- стоимость поддержки EMV-карт в процессинговом центре.

Однако при принятии решения о реализации EMV-проекта нельзя ограничиваться даже таким важным показателем, как его общая стоимость. Как правило, при осуществлении миграции существует целый ряд ограничений – хостовая (бэк-офис и фронт-офис) система была приобретена банком ранее, и вряд ли стоит ее менять, исходя только из необходимости реализации данного проекта. Также у банка уже существуют сеть оконечных устройств (терминалы, банкоматы) и персонализационное оборудование, и чаще всего целесообразнее его модернизировать, чем закупать новое.

Немаловажным является и опыт конкретных компаний-поставщиков в решении поставленных задач. Недостаток опыта реализации подобного рода проектов приводит и к затягиванию сроков ввода в эксплуатацию, и к повторным сертификациям карт, и к проблемам в сопровождении. Потеря времени может составлять до года. На каких весах можно взвесить экономию в 20% от проекта, с одной стороны, и потери времени (вместо требуемых 2–3 месяцев получилось 10) – с другой?!

Наиболее простой из стоимостных критериев – цена карты. Но и здесь, помимо цены, существуют такие показатели, как

сроки, качество тела карты и печати, надежность микросхемы и т. д.

При выборе карты и персонализационного решения следует помнить, что после запуска начнется период эксплуатации, сопровождения, развития системы. Например, миграция с одного типа карты на другой в дальнейшем может потребовать дополнительных затрат. Если банк планирует выпускать карты разных производителей или разных типов, то выпуск карт, поддерживающих общую технологию персонализации (например, CPS), позволит сократить расходы на персонализационное решение. При этом немаловажно, чтобы персонализационное решение было легко модифицируемым для поддержки новых типов карт и нового оборудования.

Рассмотрим, какие типы карт удовлетворяют тем или иным функциональным требованиям банка.

Если банк хочет выпускать карты для работы только в режиме online, то ему подойдут любые типы карт, одобренные к применению платежной системой. Ограничением в выборе карты может служить лишь необходимость разместить на карте дополнительные приложения.

В том случае, если карты предназначены для работы как в режиме online, так и в offline, либо банк внедряет карты с приложением, работающим в режиме предавторизованного дебита, то круг рассматриваемых карточных продуктов следует ограничить картами с поддержкой динамической аутентификации данных (DDA/CDA), соответствующих спецификациям EMV 2000, Visa VIS 1.4.0 или MCI M/Chip4. Международные платежные системы настоятельно рекомендуют для карт, работающих в режиме offline, использовать динамическую аутентификацию данных.

КАЛЕЙДОСКОП

Новый сервис WebMoney Transfer для социальных сетей

Система электронных Интернет-платежей WebMoney Transfer сообщила о запуске сервиса Keeper Embedded, представляющего собой платформу для обеспечения финансового взаимодействия между пользователями социальных сетей. Таким образом, владельцы социальных сетей смогут предложить пользователям легкий способ создания платежных аккаунтов внутри сообщества на базе интерфейсов Keeper Embedded.

Преимущество новой платформы состоит в том, что все технологическое и юридическое обеспечение WebMoney берет на себя. Клиенты социальных сетей получают кошельки WebMoney, с помощью которых могут передавать средства другим членам сообщества или оплачивать различные услуги. Пополнить кошелек можно несколькими способами,

в том числе с помощью предоплаченных WM-карт. Решение WebMoney предусматривает готовый биллинг при возможности интеграции интерфейса в структуру проекта. Приложение на базе Keeper Embedded уже протестировано и запущено в сети Facebook.com.

При этом эксперты не исключают возможности появления в недалеком будущем аналогичных платформ и у других платежных Интернет-систем.

Терминалы «Элекснет» начали обслуживать клиентов Банка «СОЮЗ»

С 11 марта 2008г. московские держатели карт Банка «СОЮЗ» получили возможность производить платежи в пользу банка через московскую сеть терминалов «Элекснет». Сегодня им доступны услуги пополнения текущих счетов, погашения потребительских кредитов и задолженности по счетам банковских карт. Комиссия составляет 1,5% от суммы внесенных денежных средств. ▲

Native-карты, применяемые для online/offline авторизации, не требуют большого объема памяти для хранения данных (EEPROM от 4 КБ). В качестве примера можно привести карты следующих типов:

- Gemalto Optelio D4 V14 (ранее – e-Galleon G2 DDA 4K) ;
- Sagem Orga EMV Pro Y;
- Oberthur MonetIC Chrysalis.

Все вышеперечисленные карты поставляются с предустановленными платежными приложениями VCDS или M/Chip.

Карты Global Platform (EEPROM от 18 КБ), применяемые для online/offline авторизации, – это Java Card с апплетами Visa v.2.4.1, v.2.5.1 (рекомендуется), или аналогичные апплеты от сертифицированных производителей карт. Карты с апплетом Visa v 2.4.0 также поддержи-

вают динамическую аутентификацию данных, но не удовлетворяют другим требованиям Visa по безопасности и в настоящее время удалены из списка одобренных к применению.

Карты для платежной системы MasterCard должны удовлетворять спецификации M/Chip4 Select.

В качестве примера карт Global Platform можно привести:

- Gemalto Optelio Java Dxx V14 – апплеты VSDC, M/Chip4;
- KEBT Kona 20 – апплеты VSDC, MasterCard M/Chip4;
- JCOP 21, 31 – апплеты VSDC;
- Oberthur MonetIC Cosmo DDA – апплеты VSDC, MasterCard M/Chip4.

Особое внимание хочется уделить картам, относящимся к типу Java Card «S».

Технология, названная Java Card «S», предложена компанией SUN в 2003 г. Однако массовую реализацию на картах она получила лишь в последнее время.

Карты Java Card «S» (или статические Java-карты) не позволяют загружать и удалять приложения из карты. Благодаря этому надстройка Global Platform имеет минимальный объем (например, отсутствует поддержка дополнительных Security Domain), что позволяет снизить себестоимость карты. В отличие от native-карт разработчику Java Card «S» не требуется «с нуля» разрабатывать программное обеспечение карты (ОС, приложения и т.д.), он имеет возможность разместить на карте стандартный апплет EMV-приложения, сэкономив на его разработке и отладке. За счет того что эти карты удовлетворяют требованиям спецификаций Global Platform, их выпуск осуществляется с помощью универсального персонализационного решения. Стоимость статических Java-карт эквивалентна ценам на native карты того же класса, однако в лице Java Card «S» банк приобретает тщательно отлаженный продукт со стандартной технологией персонализации.

Поставщиками чипов Java Card «S» в настоящее время являются:

- Samsung Electronics Co. Ltd - KEBT-Kona 22S, 23S (только SDA);
- NXP Semiconductors - JCOP U-10, JCOP U-20, JCOP-U30 (SDA/DDA/CDA);
- Sharp Corporation – SJCard222 (SDA/DDA/CDA).

Основным недостатком Java Card «S» является невозможность загрузки на них дополнительных приложений. На некоторых картах этого класса помимо финансового приложения производителем предустанавливается приложение лояльности.

Размещение дополнительных приложений на EMV-карте

Помимо финансового EMV-приложения на EMV-картах могут размещаться другие, в том числе небанковские бизнес-приложения. Такие приложения могут



«Яндекс.Деньги»: новый способ зачисления и вывода средств

Компания «Яндекс» предложила пользователям Интернет-системы «Яндекс.Деньги» новый способ зачисления и вывода средств. Так, клиенты получили возможность пополнить виртуальный счет или снять с него необходимую сумму через карт-счет банковской карты.

Первым банком, клиенты которого смогут воспользоваться новой услугой, стал Русский Банк Развития (РБР). Сегодня услуга доступна держателям эмитированных им карт Visa Int.

Подключить услугу «Регистрация карты в кошельке Яндекс.Денег», а также производить зачисление и вывод средств из системы «Яндекс.Деньги» с использованием карты Visa можно в сети АТМ (порядка 50 устройств) и отделений РБР (свыше 20 из которых расположены в Москве и 14 – в регионах).

Для активации услуги клиенту необходимо знать номер своего счета в Интернет-системе.

Зачисление средств на счет «Яндекс.Деньги» производится без уплаты комиссии. Комиссия за перечисление средств с виртуального кошелька «Яндекс.Деньги» на карту Visa РБР составляет 2%.

Банк Казани: первый мини-офис

Банк Казани открыл свой первый мини-офис самообслуживания – «мобильный офис». Последний представляет собой отдельно стоящий павильон, оборудованный банковскими терминалами самообслуживания.

В настоящее время «мобильный офис» Банка Казани работает в тестовом режиме. Его клиентам доступна услуга по снятию наличных и оплата услуг сотовой связи с использованием карт Visa. В дальнейшем клиентам будет предоставлена возможность вносить платежи в адрес поставщиков ряда услуг наличными. ▲

размещаться при изготовлении чипа (native и Java «S» карты) или при эмиссии и постэмиссии (Java Card, Multos). Рассмотрим основные типы дополнительных приложений и вопросы, связанные с их размещением на карте и обслуживанием.

ОТР-приложения. Приложения, поддерживающие технологию One Time Password (ОТР) и соответствующие спецификациям DPA/CAP, могут использоваться для аутентификации владельца карты путем генерации одноразового пароля в системах home banking и любых других банковских приложениях, предоставляющих доступ клиентам банка к банковским услугам.

Собственно, генерацию разового пароля может обеспечить и финансовое EMV-приложение, однако при этом в приложении на карте будут модифицироваться значения offline-счетчиков транзакций. Поэтому платежные системы рекомендуют размещать на карте отдельное специализированное EMV-приложение для генерации одноразовых паролей.

ОТР-приложение может быть размещено на картах любого типа, для этого требуется лишь небольшое количество свободной памяти (около 4 КБ EEPROM). Приложение не использует алгоритмы RSA и, соответственно, не нуждается в крипто-сопроцессоре.

На native картах ОТР-приложение должно быть персонализировано в момент эмиссии карты. На Java Card и Java Card «S» ОТР-приложение может быть размещено на карте и в режиме постэмиссии.

Как показывает практика, при реализации EMV-проектов, связанных с размещением на карте дополнительных приложений, не соответствующих стандарту EMV, возникают существенные проблемы. Авторы настоящей статьи настоятельно рекомендуют принимать их во внимание до принятия окончательного решения о целесообразности такого проекта и, соответственно, до выбора типа карты, которая сможет поддержать эти приложения.

При этом необходимо четко сформулировать следующие моменты:

1. Обоснование целесообразности и технико-экономический анализ проекта;
2. Определение возможностей карты по размещению дополнительного (не EMV) приложения;
3. Построение хостовой системы и обновление ПО терминального оборудования для поддержки дополнительного приложения;
4. Определение ролей всех участников проекта по использованию дополнительного приложения (эмитент приложения, поставщик терминального решения, сеть розничной торговли, топливные компании и т.п.);
5. Создание технологии, обеспечивающей ведение «жизненного цикла» карт и приложений.

По пункту 4 хочется особо отметить, что в случае отдельной загрузки, персонализации и управления дополнительным приложением система безопасности карты должна обеспечивать строгое разграничение доступа банка к финансовому EMV-приложению и доступа сторонней организации к дополнительному приложению.

Пункт 5 подразумевает необходимость разработки процедур восстановления и/или блокировки карты при ее утере, процедур переноса данных дополнительного приложения при перевыпуске карты, обусловленном окончанием срока действия финансового приложения, а также во многих других аналогичных ситуациях.

Приложения лояльности. Приложения лояльности или дисконтные приложения, размещенные на EMV-карте, не только «привязывают» владельца карты к определенной торговой сети, но и стимулируют его активнее пользоваться картой в качестве платежного средства в торговых точках.

Формально данные приложения поддерживаются рядом native-карт, однако из-за ограниченных возможностей по конфигурации схем лояльности на таких картах и отсутствия общепризнанных спецификаций они не получили заметно-

го распространения, несмотря на ряд запущенных проектов.

Карты Java Card «S», как правило, также содержат предустановленное приложение лояльности, но, как и на native-картах, такие приложения имеют ряд ограничений в своей функциональности.

Карты с открытой архитектурой позволяют загружать дополнительные приложения произвольной функциональности, в том числе и апплеты лояльности. Однако персонализация приложения возможна только при наличии на карте свободной памяти (EEPROM) – от 6 КБ и выше, в зависимости от конкретного приложения. Последнее замечание относится ко всем типам карт.

Топливные приложения. Это наиболее распространенный в настоящее время тип дополнительных приложений на EMV-картах. Топливные приложения могут поддерживаться рядом native-карт (например, Gemalto Optelio MPCOS R1 (ранее – MPCOS EMV R5), содержащих дополнительное приложение типа «электронный кошелек». При заказе крупных партий карт производитель может разместить на карте заказное приложение по запросу банка-эмитента.

Карты Java Card «S», как правило, не предусматривают поддержку подобных приложений (если только в качестве топливного приложения не используется дополнительный экземпляр EMV-приложения).

Карты с открытой архитектурой позволяют загружать дополнительные приложения с функциональностью, определяемой эмитентом. Требования к объему свободной памяти (EEPROM) в случае топливных приложений аналогичны требованиям к размещению приложений лояльности.

Приложения для безопасного хранения произвольных данных. Привлекательность приложений такого рода состоит в том, что они разработаны на основании спецификаций платежных систем:

- Visa – Visa Smart Secure Storage (V3S);

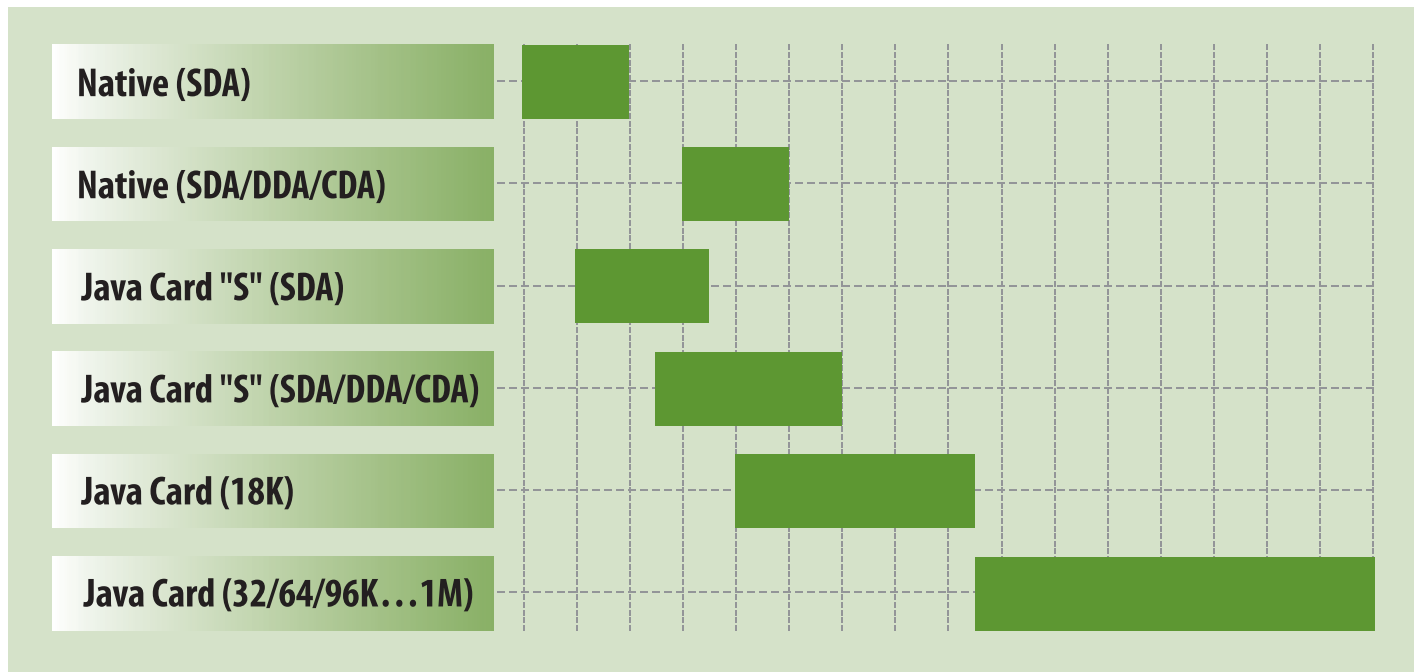


Рис. 1. Соотношение цен на EMV-карты различных типов

- MasterCard – MasterCard Open Data Storage (MODS).

Соответственно, документация по приложениям доступна участникам каждой из этих платежных систем и является де-факто внутриотраслевым стандартом.

Приложения могут использоваться для хранения идентификационных данных владельца, истории лояльности владельца карты, криптоматериала и т. п.

Приложения могут быть предустановлены производителем на native-картах либо загружены в качестве дополнительных апплетов на Java-карты.

Объем занимаемой приложением памяти зависит от объема хранимых в нем данных.

Социальное приложение. Очень широкое толкование данного термина не позволяет с точностью утверждать, на каких именно типах карт оно может быть реализовано. Во многих случаях native-карты, имеющие приложение типа «электронный кошелек», способны поддерживать функциональность социального приложения. В других случаях можно использовать приложения MODS или V3S. Очевидно, что полнофункциональные Ja-

va Card позволяют загрузить социальное приложение любого типа, если это позволяет сделать объем свободной памяти карты (EEPROM).

Транспортные приложения. В российских проектах для транспортных приложений, как правило, используют бесконтактные карты с технологией Mifare. Имеются 2 варианта совмещения транспортного бесконтактного приложения с контактным EMV-приложением. Более простыми в изготовлении являются гибридные карты (2 чипа, 2 интерфейса). В частности, это может быть любой контактный EMV-чип, которой имплантируется на бесконтактную карту Mifare.

Бесконтактные приложения MasterCard PayPass и Visa payWave. Данные приложения предназначены для осуществления «быстрых» платежей, могут использоваться на транспорте и в торговых сервисных точках, требующих быстрого обслуживания клиентов, например, в сетях ресторанов быстрого обслуживания.

Существует несколько разновидностей бесконтактных карт. Простейшая – это бесконтактные карты с образом магнитной полосы на чипе.

Имеются также комбинированные Java-карты (2 интерфейса, 1 чип). Например, у Gemalto это карты Optelio Contactless (GCX-4 для PayPass и Palmera Air для payWave). Стоимость этих карт заметно выше, чем карт с одним бесконтактным интерфейсом, но они могут полностью персонализироваться через контактный интерфейс, что позволяет минимизировать инвестиции в систему персонализации (как в оборудование, так и в программное обеспечение). Используя специальный апплет, эмулирующий Mifare, такие карты могут обеспечивать функционирование транспортного приложения по ранее внедренной технологии.

Соотношение цен на карты различных типов

Приводить абсолютные ценовые значения на карты весьма затруднительно, т. к. во многих случаях эта информация является конфиденциальной. Абсолютные цифры зависят от размера партии поставки и множества других причин. Тем не менее попытаемся проиллюстрировать соотношение цен на карты различных типов (см. рис. 1).

В связи с тем что наличие крипто-сопроцессора заметно влияет на цену EMV-карты, в нашей диаграмме цены на карты native и Java «S» приведены отдельно для продуктов без сопроцессора (SDA) и для карт с сопроцессором (SDA/DDA/CDA). Полнофункциональные Java-карты, как правило, обладают крипто-сопроцессором (исключение составляют 3–4 типа карт, включая JCOPIV10), и в диаграмме деление этого типа карт на подклассы выполнено по другому параметру – объему памяти EEPROM. Java-карты с памятью 18 КБ позволяют реализовать базовое финансовое приложение и, возможно, OTP-приложение в качестве дополнительного. Фактически возможности такой карты эквивалентны возможностям карт типа Java Card «S». Карты с памятью 32 КБ и более позволяют загружать на карту произвольные дополнительные приложения, но и цена их резко отличается в большую сторону от всех других типов карт.

Как демонстрирует диаграмма, в настоящее время цены на native-карты и карты Java Card «S» одинаковой функциональности практически не различаются, что должно стимулировать распространение карт типа Java Card «S» на мировом рынке.

Мы преднамеренно исключили из рассмотрения карты с бесконтактным интерфейсом, т.к. это снизило бы наглядность диаграммы. Можно лишь отметить, что использование в карте двух интерфейсов, контактного и бесконтактного, практически удваивает цену карты.

Влияние функциональности карты на процедуры сертификации

Особенности функционирования EMV-приложения на карте определенного типа необходимо учитывать при заполнении сертификационных форм платежной системы.

При прохождении сертификации необходимо заполнить соответствующие формы – Visa Personalization Assistant (VPA)

или CPV Issuer Form (MasterCard), где в первую очередь определяются базовые функциональные возможности карты и способы ее обслуживания банком-эмитентом. При определении набора параметров карты необходимо контролировать их номенклатуру, сверяясь с документацией поставщика карт.

В VPA (Visa) пользователь определяет класс, к которому относится карта: native или Java Card, затем перечисляет поддерживаемые картой функции (AIP). Последующий набор вопросов, задаваемых в VPA, в значительной степени зависит от ранее данных ответов. Формируемые выходные файлы VPA не содержат всех обязательных для персонализации данных, а только те величины, которые контролируются при сертификации.

Помимо сравнения результатов заполнения VPA с тестовой картой, карта проверяется с помощью Card Validation Tool (в настоящее время используется продукт компании Collis) на достаточность и непротиворечивость данных.

В CPV-форме (MasterCard) ключевым является тип платежного продукта, размещаемого на карте, и набор проверок полномочий владельца карты. Шаблоны, описанные в документах MasterCard, допускают от 1 до 4 наборов проверок, в зависимости от типа платежного продукта. Некоторые элементы данных имеют предопределенные значения в зависимости от выбранного шаблона.

Сертификация в MasterCard выполняется в два этапа (которые могут быть совмещены по времени):

КАЛЕЙДОСКОП

Фишинговые атаки становятся все более изощренными

Согласно данным «Отчета по мошенничествам в Интернете» (Online Fraud Report) компании RSA Security за февраль 2008 г., преступники продолжают совершенствовать свои компьютерные атаки на кредитно-финансовые учреждения.

Одна из тактик состоит в использовании множества вариантов одного фальшивого web-адреса банка в различных фишинговых письмах с целью обойти антиспамовые фильтры электронной почты. Фальсифицированный URL банка, внешне похожий на реальный банковский сайт, используется в фишинговой рассылке для незаконного получения паролей и других персональных данных адресатов.

Еще один тактический ход – использование запутанных или закодированных фишинговых комплектов (автоматизированных инструментов, позволяющих мошенникам проводить фишин-

говые атаки), которые сложно обнаружить. Данные комплекты препятствуют исследованию уровня безопасности Интернет-среды.

По данным RSA Security, преступники стали уделять пристальное внимание кредитно-финансовым учреждениям, ранее не подвергавшимся нападениям. Выросло число атак на южноамериканские банки. В феврале 2008 г. к списку стран, подвергшихся наибольшему количеству нападений, впервые присоединились Ирландия и Бразилия, а в США мошенники атаковали 20 новых банков. В том же месяце мишенью фишеров стал ряд банков Великобритании. За прошедшие 4 месяца RSA идентифицировала пять новых фишинговых сетей, которые используют зараженные компьютеры для нападения на кредитно-финансовые учреждения во всем мире. Самый печально известный пример – использование так называемого Storm Botnet (центрального пункта управления компьютерной сетью, контролируемой хакерами) для проведения фишинговых атак с зараженных компьютеров. ▲

- контроль данных, заполненных в CPV-форме;
- проверка работоспособности тестовой карты и ее соответствие CPV-форме.

Процесс сертификации EMV-карт в платежной системе требует особой аккуратности. Мы настоятельно рекомендуем перед отсылкой карты на сертификацию провести тестирование карты на

предмет ее соответствия параметрам, указанным в сертификационной форме, и необходимым бизнес-требованиям.

Заключение

Очевидно, что в рамках журнальной публикации невозможно дать рекомендации по выбору типа EMV-карты на все случаи жизни. В каждом конкретном случае свое

влияние на окончательное решение оказывают множество факторов. Поэтому целью авторов настоящей статьи было поделиться с эмитентами практическим опытом, полученным в течение 5 лет на десятках реализованных проектов, предложить некоторые пути по выбору рационального решения и предостеречь от часто повторяемых банками ошибок. ПЛАС

КАЛЕЙДОСКОП

Новый продукт «Доктор Веб» для крупных корпораций

Компания «Доктор Веб» объявила о выпуске нового продукта – Dr.Web для IBM Lotus Domino, – предназначенного для обеспечения защиты от вирусов, любого рода вредоносных объектов и спама в системах IBM Lotus Domino. Последние, как правило, используются крупными и средними корпорациями. Как заявил генеральный директор компании «Доктор Веб» Борис Шаров, системы антивирусной защиты, особенно в сочетании с антиспамом, давно стали не только средством защиты, но и средством экономии. Руководители крупных компаний, в которых сбой в функционировании информационных систем оборачивается убытками, именно в этой плоскости рассматривают приобретение антивируса. В перечне бизнес-задач, которые позволяет решать продукт Dr.Web для IBM Lotus Domino, – кардинальное решение проблемы спама, снижение затрат компаний на восстановление данных, потерянных из-за атак спамеров и хакеров, уменьшение финансовых потерь из-за простоев, вызванных действиями вредоносных объектов, снижение риска потери важных данных и накопленной информации, устранение возможности утечки конфиденциальной информации.

При этом новый продукт компании «Доктор Веб» чрезвычайно прост в раз-

вертывании и легко масштабируем, не требуя значительных временных затрат при внедрении.

Прием платежей за использование ГЛОНАСС в сети КиберПлат

Система Интернет-платежей КиберПлат предоставила возможность производить оплату использования ручных и автомобильных навигаторов глобальной навигационной системы ГЛОНАСС в сети приема платежей, обслуживаемых системой.

Формирование потребительского сегмента является сегодня приоритетным направлением развития системы ГЛОНАСС. Так, уже в ближайшее время технологии ГЛОНАСС выйдут на массовый рынок и будут доступны населению. Предполагается, что основным направлением использования ГЛОНАСС населением будет определение местонахождения и составление маршрутов с помощью ручных и автомобильных навигационных устройств. При этом коммерческое использование системы в данном сегменте, а также в сегменте обеспечения безопасности эксплуатации автомобильного транспорта (контроль маршрута, защита от угона и др.) будет развиваться наиболее быстро.

Сеть пунктов приема платежей CyberPlat (КиберПлат) насчитывает более 115 000 точек, подключенных к системе напрямую, с точками приема субдилеров ее размеры составляют около 160 тыс. точек, расположенных по всей

территории России и в ряде стран СНГ. Обширная инфраструктура приема платежей позволит пользователям ГЛОНАСС оплачивать ее услуги в любом удобном для них месте.

В Киеве парковку можно оплатить с мобильного телефона

Как сообщает пресс-служба Киевской городской государственной администрации (КГГА), с начала апреля 2008 г. в Киеве стартовал проект «Мобильная парковка», охвативший 22 парковочные площадки. В его рамках расчеты за услуги парковки автомобилей можно производить при помощи мобильного телефона.

Водитель, купив специальную скретч-карту и отправив SMS-сообщение на указанный номер, осуществляет открытие или пополнение парковочного счета. В настоящее время скретч-карты распространяются коммунальным предприятием «Киевтранспарксервис» и доступны через сети автозаправочных станций «Лукойл-Украина», «Кло», сети киосков «Союзпечать», «Укрпочты», а также в кассах Киевского метрополитена.

Перед началом парковки водитель также должен отправить SMS-сообщение с указанием номера парковочной площадки и своего автомобиля. Как отмечает первый заместитель председателя КГГА Денис Басс, после введения системы безналичной оплаты за услуги парковки сумма поступлений в бюджет от данного направления возросла в 10 раз. ▲