

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

2-3 апреля 2008 г.

Кохно Вадим,
Паничкин Алексей,
Сахаров Дмитрий



Обсуждаемые вопросы

- Определение терминологии и классификации
- Цели EMV-миграции
- Связь между возможностями карты и особенностями работы EMV приложения
- Подходы к выбору карты
- Влияние функциональности карты на процедуры сертификации
- Помощь от Пронит, накопленный опыт

Определение терминологии и классификации

- **Тип операционной системы:**
 - с открытыми операционными системами (Java Card, .Net Card и Multos),
 - с операционной средой, разработанной производителем для конкретного продукта - native (или proprietary) карты.
- **Наличие или отсутствие криптопроцессора, обеспечивающего несимметричную RSA криптографию:**
 - карты со статической аутентификацией (SDA),
 - карты с динамической и/или комбинированной аутентификацией (DDA/CDA), которые, как правило, также поддерживают зашифрованный PIN.
- **Интерфейс к обслуживающим устройствам (устройствам чтения/записи):**
 - контактные карты,
 - бесконтактные карты,
 - комби-карты (два интерфейса к одному чипу).
 - гибридные карты (с двумя чипами - контактным и бесконтактным).
- **Возможность «стандартной» персонализации:**
 - карты и приложения, поддерживающие CPS,
 - карты и приложения, для которых требуется специфическая программа персонализации.
- **Возможность загрузки дополнительных приложений:**
 - «статические» карты (native и Java Card "S"),
 - «динамические» карты (Java Card и Multos).

Цели EMV-миграции

- Сертификация в платежной системе, начальный опыт в работе с чиповыми картами, минимизация затрат на приобретение карт;
- Поддержка работы карты в режиме offline, преавторизованный дебет;
- Предоставление клиентам услуг home banking и аналогичных, поддержка технологии одноразовых паролей CAP/DPA;
- Эмиссия карт с дополнительным приложением: лояльности, топливным приложением, «электронным кошельком», социальным приложением, транспортным приложением;
- Пост-эмиссия приложений;
- Обслуживание карт через бесконтактный интерфейс по технологии PayPass или PayWave.

Связь между возможностями карты и особенностями работы EMV приложения

Соответствие EMV-приложения на карте определенной спецификации платежной системы не обеспечивает поддержку всех описанных функциональных возможностей, а лишь гарантирует непротиворечивость приложения указанной спецификации.

Набор параметров, необходимый для реализации одной и той же функциональности, может зависеть от типа карты

При выборе типа карты с EMV-приложением следует учитывать:

- Ограничения функциональных возможностей карты, накладываемые производителем карт (возможности чипа);
- Ограничение номенклатуры EMV-карт, вносимое платежной системой (Approval ID карты с конкретным приложением);
- Ограничения функциональных возможностей приложения задаваемые банком-эмитентом (Online/Offline, контроль международных и иновалютных операций по карте, географические ограничения обслуживания карты).

Подходы к выбору карты

Минимизация стоимости EMV-решения при условии выполнения сформулированных бизнес-требований и учетом дальнейшего развития системы. Стоимость решения включает:

- стоимость EMV-карты;
- цена за сертификацию карты в платежной системе;
- стоимость персонализационного решения;
- стоимость поддержки EMV-карт в процессинговом центре.

Следует помнить, что все вышеперечисленные пункты могут в дальнейшем потребовать дополнительных затрат при миграции с одного типа карты на другой.

Подходы к выбору карты

Карты для работы только в режиме Online

Любые типы карт, одобренные к применению платежной системой.

Карты для работы в режиме Offline, преавторизованный дебит

Карты с поддержкой динамической аутентификацией данных (DDA/CDA), соответствующие спецификациям EMV 2000, Visa VIS 1.4.0 или MCI M/Chip 4.

Native карты (EEPROM от 4K)

- GamAlto e-Galleon G2 DDA 4K (Optelio D4 V14) – Visa, MCI
- Sagem-Orga EMV Pro Y (CPS) – Visa, MCI
- Oberthur MonetIC Chrysalys – Visa, MCI
- ...

Карты Global Platform (EEPROM от 18K)

- Java Card с апплетами Visa v.2.4.1, v.2.5.1, ... или аналогичные от других разработчиков, MCI M/Chip 4.*
- GemAlto GXP 4 (Optelio Java Dxx V14) - Visa, MCI
 - KEBT Kona 20 - Visa, MCI
 - JCOP 21, 31 – Visa
 - Oberthur MonetIC Cosmo DDA – Visa, MCI
 - ...

Карты Java Card "S"

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

Java Card "S" или статические Java-карт 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 не требуется «с нуля» разрабатывать ПО карты, он имеет возможность разместить на карте стандартный апплет EMV-приложения, сэкономив на его разработке и отладке.

Поставщики Java Card "S":

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

Подходы к выбору карты (дополнительные функции)

Поддержка технологии One Time Password (OTP), соответствующей спецификациям DPA/CAP

Может использоваться основное финансовое приложение карты, однако платежные системы рекомендуют создавать на карте второе специализированное приложение со специальным AID.

На Native и Java "S" картах дополнительное приложение должно быть отперсонализировано в момент выпуска карты.

На Java Card OTP-приложение может быть размещено на карте и в режиме post-issuing.

Не использует алгоритмы RSA.

Необходим минимальный объем дополнительной памяти (EEPROM) для размещения второго приложения

Подходы к выбору карты (дополнительные функции)

Проблемы обсуждаемые при запуске проекта по размещению на карте дополнительных приложений

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

Подходы к выбору карты (дополнительные функции)

Поддержка приложений лояльности

Формально поддерживаются рядом Native-карт, однако из-за ограниченных возможностей по конфигурации схем лояльности не получили заметного распространения.

Java Card "S", как правило, также содержат загруженное приложение лояльности, но как и в Native-картах приложения имеют ряд ограничений в своей функциональности.

Карты с открытой архитектурой позволяют загружать дополнительные приложения произвольной функциональности, в том числе и Loyalty. Однако размещение приложения возможно только при наличии в карте свободной памяти (EEPROM) – от 6К и выше, в зависимости от конкретного приложения.

Подходы к выбору карты (дополнительные функции)

Поддержка топливных приложений

Поддерживаются рядом Native-карт (MPCOS-EMV, ...) имеющих дополнительные приложения типа «электронный кошелек».

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 произвольной функциональности. Требования к объему свободной памяти (EEPROM) аналогичны требованиям к приложениям лояльности.

Подходы к выбору карты (дополнительные функции)

Приложения для безопасного хранения произвольных данных

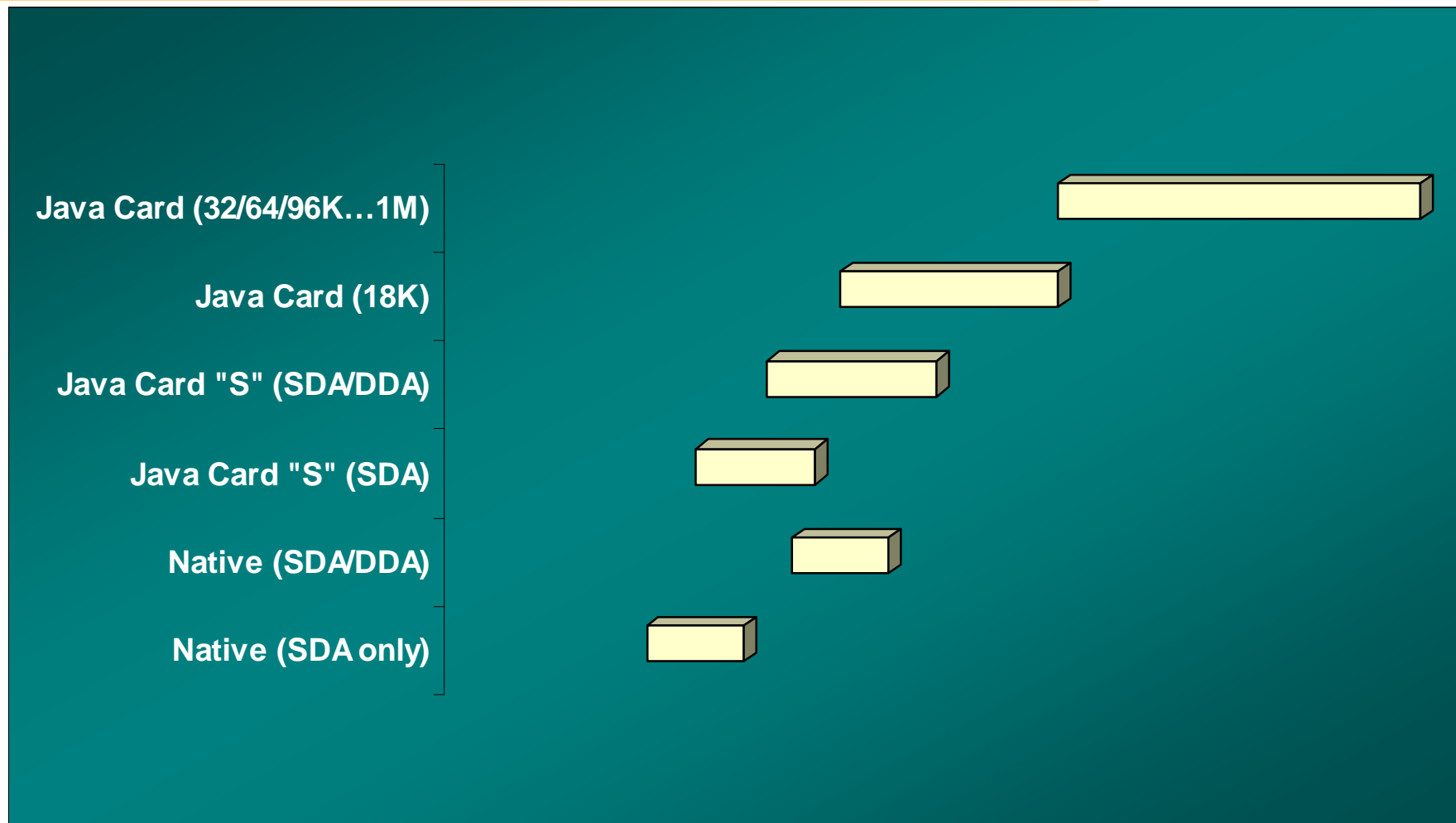
Разработаны на основании спецификаций платежных систем:

- Visa – Visa Smart Secure Storage (V3S);
- MasterCard - MasterCard Open Data Storage (MODS).

Могут использоваться в качестве хранения идентификационных данных владельца, истории лояльности владельца карты, криптоматериала и т.п.

Приложения могут быть реализованы производителем на Native-картах, либо загружены в качестве дополнительных апплетов на Java-карты.

Соотношение цен на EMV-карты различных групп



Влияние функциональности карты на процедуры сертификации

При прохождении сертификации необходимо заполнить соответствующие формы (VPA или CPV), где в первую очередь определяются базовые функциональные возможности карты и способы ее обслуживания банком –эмитентом.

В **VPA** (Visa) пользователь определяет класс карты: Native или Java, а затем перечисляет поддерживаемые картой функции (AIP). 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 на достаточность, непротиворечивость данных.

Влияние функциональности карты на процедуры сертификации (продолжение)

В **CPV**-форме (МСІ) ключевым является тип платежного продукта, размещаемого на карте и набор проверок полномочий владельца карты. Шаблоны, описанные в документах МСІ допускают от 1 до 4 наборов проверок, в зависимости от платежного продукта. Значения некоторых элементов данных имеют детерминированные значения в зависимости от выбранного шаблона.

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

- Контроль данных, заполненных в CPV-форме;
- Проверка работоспособности тестовой карты и ее соответствие CPV-форме.

Помощь от ПРОНИТ, накопленный опыт

Компания ПРОНИТ предлагает помощь и осуществляет сопровождение при прохождении сертификации смарт-карт в международных платежных системах Visa и MasterCard.

Мы предлагаем три варианта взаимодействия с заказчиком при прохождении сертификации:

- Специалисты ПРОНИТ на основании пожеланий Банка определяют значения всех параметров EMV-продукта, выполняют технологические действия по заполнению сертификационных форм. Проверяют работоспособность тестовой карты;
- Специалисты ПРОНИТ консультируют сотрудников Банка при выборе значений параметров EMV-продукта и заполнении форм;
- На основании подготовленных специалистами Банка форм, ПРОНИТ осуществляет настройку системы подготовки данных.

В любом случае заказчику направляется план выполнения работ по прохождению сертификации.

Ежегодно сотрудники компании сопровождают прохождение 20-30 сертификаций EMV-карт в международных платежных системах. Подавляющее количество сертификаций завершается успешно с первой попытки. Накопленный опыт позволяет избежать нам ошибок, которыми часто сопровождается процедура сертификации.

Собственное ПО тестирования EMV-приложений (**EMV Insight**) позволяет нам проверять персонализационные данные на этапе их подготовки, заполнения VPA и CPV форм, выпуска тестовых и рабочих карт с EMV-приложениями.

Ваш Верный Выбор



Контактная информация

- Веб-сайт: <http://www.pronit.ru>
- E-mail: pronit@pronit.ru
- Тел./факс: +7 (495) 221-60-33
+7 (495) 589-27-25
- Адрес: 121357, г. Москва,
ул. Вересаева, 15

