Из книги «Пластиковые карты», 5-ое издание,
Москва, Издательская группа «БДЦ-пресс», 2005 г.

Перлин Ю.В., Сахаров Д.В., Товб Ю.С.

Персонализация микропроцессорных карт спецификации EMV. Общий подход и промышленное решение

В настоящем разделе рассматриваются вопросы персонализации прежде всего микропроцессорных банковских карт международных платежных систем, хотя описываемые подходы и программные решения легко можно распространить (что нами уже в целом ряде случаев сделано) не только на карты различных локальных платежных системы, но и на идентификационные карты с микросхемой (например, водительские удостоверения, партийные билеты, страховые полисы), на SIM-карты для мобильных телефонов, транспортные и «бензиновые» карты и т. д.

1. История вопроса

Как давно это было… Наверное, именно прошлый и этот год знаменательны десятилетними юбилеями первых российских платежных систем на смарт-чип-картах. В то время вовсю еще шли споры, а можно ли отнести к смарт-картам карты памяти или нельзя, выбор карты часто определялся не ее функциолнальностью и защищенностью, а только ценой и простотой программирования чипа. Но системы такие были востребованы и появлялись буквально десятками. Иных уж нет. Иногда к глубочайшему сожалению. Так, например, прекратила свое существование система «Полискарт», к созданию которой имели непосредственное отношение авторы. А ведь это была чуть ли не первая в мире система с реальным использованием микропроцессорных карт с шифрованием, с off-line обслуживанием карт в банкоматах. Зато другие «ровесники» – Сберкарт, Золотая Корона, Аккорд в добром здравии и вовсю процветают.

Миллионы микропроцессорных карт выпущены существующими и существовашими платежными системами. Стало быть, как-то все эти миллионы карт были проперсонализированы. Но даже с большой натяжкой все использованные для этих целей способы персонализации нельзя назвать «промышленными». Очень часто на карту просто наносился (наносится) номер, затем карта руками оператора вставляется в ридер или терминал. Все, персонализация закончена. Как говорил один многоуважаемый коллега, «зачем мне эмбоссер, я лучше найму два десятка студентов, пусть по ночам работают, а не гуляют…». И с точки зрения уровня автоматизации, производительности, использования передовых технологий, наконец, возник парадокс – в области персонализации «находящиеся на самом передовом крае» смарт-карты значительно проигрывали традиционным, известным с «незапамятных» времен, то есть уже несколько десятилетий, картам с магнитной полосой. Правда, эмиссия этих карт насчитывала не миллионы, а если брать «в мировом масштабе» десятки миллиардов штук. Ведь технологии персонализации магнитных карт разрабатывались благодаря, в том числе, таким гигантам как Visa и Mastercard.

Новые времена - новые проблемы. Visa и Mastercard не торопились. Но шла разработка международных ISO-стандартов для карт с микропроцессором, общих спецификаций – спецификаций EMV, собственных спецификаций платежных систем – VSDC (Visa) и M/Chip (Mastercard). В тот момент, когда стало ясно, что переход этих платежных систем на микропроцессорные карты неотвратим, встала задача распространить универсальность и технологичность персонализации магнитных карт на карты с микропроцессором. И задача эта оказалось очень и очень непростой. В том числе и потому, что если практически полностью специфицировано «общение» EMV-карты и платежного терминала, то до сих пор нет строгих законченных требований, как эти карты должны персонализироваться.

2. О чем, собственно, речь?

По мнению самих платежных систем самое трудное в так называемой EMV-миграции – это именно персонализация. И этот сложный вопрос, как нам кажется, требует достаточно детального рассмотрения.

В процессе персонализации участвуют:

- собственно карта с микросхемой,
- персонализационное устройство,
- данные, помещаемые на карту,
- программное обеспечение для управления всем процессом.

Таким образом, прежде всего, надо иметь представление о различных EMV-картах, чем отличаются друг от друга, как производятся, когда и где персонализируются.

Необходимо также понимать, как необходимо преобразовать знакомую технологию персонализации банковских магнитных карт, в том числе как модернизировать имеющееся персонализационное оборудование.

Какие данные помещаются на карту, как их подготовить, как наиболее рационально персонализировать карты. При этом надо исходить из того, что сегодня надо персонализировать одни карты, а завтра другие, сегодняшний тираж ограничен несколькими тысячами карт, а завтра их будет несколько сотен тысяч, что потребует использовать совершенно иное по производительности оборудование. И с этих точек программное обеспечение должно обладать высокими адаптивными качествами. Кроме того желательно иметь инструмент, позволяющий проверить правильно ли карты персонализированы, убедиться в том, что данные, записанные в микросхему соответствуют исходным, посмотреть как поведет себя карта в диалоге с терминальным устройством.

3. Функциональные и технологические типы карт

Карты, удовлетворяющие спецификации EMV (EMV означает Europay-Mastercard-Visa), отличаются от других микропроцессорных платежных карт (таких, например, как «электронные кошельки») тем, что для них строго регламентирвана последовательность совместного функционирования с приемными устройствами (терминалами). Это последовательность (некоторые шаги опциальны и могут быть опущены) состоит из следующих шагов:

- Выбор приложения (команда Select). Терминал запрашивает карту о том, каие приложения она поддерживает (например, Cirrus и локальное), и если

имеются совпадения с приложениями, которые поддерживает сам терминал, выбирается одно из них.

- Запрос терминалом основных сведений о приложении (команда Get Processing Option). Карта выдает основную информацию о приложении, в частности, какую функциональность поддерживает и структуру хранения данных выбранного приложения.
- Чтение данных приложения (команда Read Record). На основании информации о структуре файлов с данными, полученными на предыдущем шаге, терминал читает эти данные.
- Аутентификация данных (Data Authentication). Терминал в режиме off-line проверяет, что данные, прочитанные с карты, истинные и не подвергались ранее подделке или незаконному исправлению. Существуют следующие способы аутентификации: статическая (SDA), динамическая (DDA) и клон-усовершенствование динамической– комбинированная (CDA).

Несколько упрощенно суть простейшей, статической, аутентфикации заключается в следующем. В процессе выпуска карт банк-эмитент создает пару несимметричных ключей. Публичный ключ отправляется в Центр сертификации данной платежной системы, откуда возвращается подписанным секретным ключом системы. Пара - публичный ключ и его сертификат загружаются на карту. В то же время часть данных (несекретных, но наиболее чувствительных по мнению системы и эмитента) подписываются секретным ключом банка-эмитента. Платежный терминал, зная публичный ключ системы, прочитав с карты публичный ключ эмитента и его сертификат, убеждается в том, что этот публичный ключ неподдельный. А зная публичный ключ эмитента и сертификат подписанных данных, может убедиться в том, что и они не претерпели изменения с момента выпуска карты. Таким образом, последовательно терминал дважды проверяет истинность информации прочитанной с карты – сначала истинность публичного ключа банка, затем истинность данных.

В процессе выполнения DDA и CDA используется команды Internal Authentication и Generate Application Cryptogram. Суть используемого алгоритма заключается, в том, что данные карты, а также «динамические» характеристики транзакции, такие как показатель счетчика транзакций карты и случайное число, выдаваемое в карту терминалом, подписываются секретным RSA-ключом, индивидуальным для каждой карты. В свою очередь, парный этому ключу публичный ключ подписывается секретным ключом эмитента (аналогично тому, как в SDA публичный ключ эмитента подписывается секретным ключом платежной системы). Подтвержденное центром доверия (в данном случае это банк-эмитент) знание публичного ключа карты достаточно, чтобы убедиться в правильности криптограммы. Таким образом, в DDA и CDA по сравнению по SDA возникает как бы третий (дополнительный этап). Если в SDA сначала проверяется истинность публичного ключа эмитента, а зетем истинность «статических» данных, то в рассматриваемых случаях, после проверки истинности публичного ключа эмитента, убеждаемся в истинности публичного ключа карты, а затем «статических» и «динамических» данных карты и терминала.

- Проверка ограничений на использование карты (Processing Restrictions). Терминал анализирует полученную ранее от карты информацию и определяет может ли она быть обслужена в это время, в этом географическом месте, в данной торговой точке (по типу) и т. д.

- Проверка полномочий владельца карты (Cardholder Verification). Среди данных, прочитаных с карты, находятся и параметры, определяющие каим образом осуществляется проверка лица, предъявившего карту). Наряду с известными для случая магнитной карты таких методов, как подпись клиента и проверка PIN в режиме on-line, используется также off-line проверка PIN.

Для обеспечения этой процедуры сначала проверяется не превышен ли лимит неудачных попыток ввода, а затем, если все в порядке вводится и сам PIN (команда Verify). При этом существует 2 способа ввода – обычный (plaintext) и шифрованный. Во втором случае ПИН шифруется с использованием публичного RSA-ключа карты с использованием случайного картой выданного числа и расшифровывается внутри карты секретным ключом. При этом возможно использование пары ключей для DDA, а возможно и наличие отдельной пары для PIN-шифрования.

Понятно, что и DDA, и -шифрованный PIN предъявляют к карте одинаковые требования, а именно поддержку RSA-шифрования. Таким образом, оба этих функционала связаны – если карта не может поддержать DDA, нечего говорить о шифровании PIN, и т. д.

- Проверка рисков (Terminal Risk Management). Терминал проверяет не находится ли карта в «черном» списке, превышен ли floor limit, превышает ли величина транзакции лимит по обслуживанию карты в режиме off-line, требуется ли обязательно послать on-line запрос и т. д.
- Принятие терминалом решения о дальнейших действиях (Terminal Action Analysis). На основании приведенных ранее операций (аутентификации данных, проверки ограничений на использование, проверки off-line PIN, проверки рисков), терминал принимает решение, как ему поступить с транзакцией. Имеется три варианта – отклонить транзакцию, послать транзакцию за авторизацией в режиме on-line, принять транзацию off-line. Терминал предлагает карте (команда Generate Application Cryptogram - AC) вычислить 3DES-криптограмму переданного запроса. В соответсвии с перечисленными вариантами решений имеются и три типа криптограмм - Application Authentication Cryptogram (AAC), Authorization Request Cryptogram (ARQC), Transaction Certificate (TC).
- Принятие картой решения о дальнейших действиях (Card Action Analysis). На основании заданной эмитентом логики поведения и значений параметров, получив запрос на криптограмму, карта сначала сама анализирует приятые риски. При этом, решение, предложенное терминалом, картой может быть только ужесточено. То есть решение послать on-line запрос можент быть либо подтверждено, либо пересмотрено на отклонение транзакции сразу, решение терминала о принятии транзакции в off-line режиме может быть принято или заменено на отклонение транзакции или на on-line запрос. В соответсвии с решениемм карты формируется криптограммы типа AAC, ARQC или TC.
- Авторизация карты в режиме on-line (Online Processing). Если терминал и карта приняли решение послать эмитенту on-line запрос, то терминал по линиям связи передает криптограмму ARQC и данные карты и транзакции, использованные при ее получении. Хостовая система банка-эмитента проверяет корректность криптограммы (используя уникальный 3-DES ключ карты), принимает решение по данной транзакции и посылает ответ с критограммой типа Authorization Response Cryptogram (ARPC), используя

тот же ключ карты. В случае, если хостовая система поддерживает изменение данных на карте методом скриптов, в ответе посылается соответствующий скрипт.

Если карта поддерживает аутентификацию эмитента, то терминал, получив авторизационные данные, посылает их в карту, используя команду External Authentication. Карта при этом вычисляет значение ARPC и сравнивает с полученным от терминала. Если все сходится, значит ответ пришел от эмитента. Если аутентификация не прошла, то следующие транзакции будут отправлены в on-line до успешного сравнения ARPC. Эмитент имеет возможность установить на карте параметр, отклоняющий транзакию в случае неудачной аутентификации.

- Изменение параметров карты (Issuer-to-Card Script Processing). Эмитент имеет возможность путем посылки в авторизационном ответе специальных скриптов изменить параметры карты, используемые при работе в off-line, а также PIN и число попыток его предъявления, заблокировать или разблокировать приложение, заблокировать карту. Скритпы подписываются с использованием специального 3DES-ключа карты, новое значение PIN шифруется таким же ключом.
- Завершение процесса (Completion). На основании информации, полученной от эмитента, транзакция либо принимается, либо отклоняется. Соответственно формируются криптограммы TC или AAC.

На рынке существует достаточно широкая номенклатура сертифицированных карт, удовлетворяющих спецификациям EMV и международных платежных систем. Попробуем классифицировать эти предложения. Обратим внимание на тот факт, что если достаточно полно описаны поведение карты «в бою» (при работе с терминалом), то вопросы (и команды), касающиеся персонализации карты отданы «на откуп» разработчикам чипов и самих карт.

Существуют два типа карт – карты с «закрытыми» операционными системами (т.н. proprietary или native карты) и карты с открытыми ОС.

Как правило, операционные системы (маски) для native карт разрабатывают сами производители смарт-карт, в первую очередь, такие крупные как Gemlpus, Axalto, Oberthur, G&D. В этих картах приложение – это двухуровневая структура данных (ПК-аналог - файлы внутри директории). По своим функциональным возможностям данные карты можно разделить на карты только с одним EMV-приложением (VSDC или M/Chip Lite) и мгогофункциональные карты. Преимущество первых – относительная дешевизна, вторых – возможность использования дополнительных приложений. В простейшем случае это может быть приложение типа «loyalty» - приложение, обеспечивающее поощрение клиентов при обслуживании в определенной торговой сети путем начисления премиальных баллов (бонусов), величина которых, как правило, зависит от величины покупки. Кроме того, возможно создание как бы дополнительных локальных EMV-приложений, аналогичных приложениям платежных систем (здесь, правда, может возникнуть проблема урегулирования такого решения с самой международной платежной системой). Наконец, с помощью ряда карт можно строить различные “кошельковые” схемы, в том числе хорошо известные в России системы предавторизованного дебета или “бензиновые” системы типа “электронный кошелек”, а также различные идентификационные системы (пенсионный фонд, медицинское

страхование, логический доступ в корпоративные сети, физический доступ и т.д.). В подавляющем большинстве чипы этих карт не имеют крипто-процессора и не поддерживают динамическую аутентификацию и шифрованный PIN (хотя имеются и исключения).

К картам с открытыми ОС относятся Java-карты (или близкие к ним карты, удовлетворяющие спецификациям Global Platform) и карты с операционной системой Multos. Приложения на данных картах – программы (апплеты), обеспечивающие ту или иную функциональность. При активизации апплета возникает возможность записи и хранения данных. На картах Multos реализуется приложение M/Chip Select, принадлежащее Mastercard. Карты поддерживают DDA.

Карты Global Platform могут быть как с поддержкой DDA и шифрованного PIN (то есть с крипто-процессором), так и поддерживающие SDA. Как правило, для этих карт существует только апплет VSDC, предназначенный для выпуска карт Visa. Однако у некоторых карточных производителей имеются апплеты и для Mastrecard (M/Chip Lite – SDA-карты). Среди сертифицированных карт Global Platform с поддержкой DDA (производители карт –правообладатели на ОС - Oberthur, G&D и Gemplus) стоит отметить карты JCOPx0 (x=2,3), правообладателем которых яляется сама Visa, передающая право изготавливать карты на достаточное больше число производств и регулирующая конечную цену). Карты Global Platform интересны также с точки зрения персонализации. Для этих карт существуют строгие рекомендации по механизму персонализации и структуре персонализационного файла (спецификация Common Personalization). Следует отметить, что следование данной спецификации удобно и целесообразно при персонализации любых карт.

Карты с открытыми ОС – многофункциональные, более того, и предназначены, в основном, для многофункциональных систем, более дорогие, нежели proprietary карты. Некоторые из них способны безопасно поддержать так называемую пост-эмиссию, когда приложение не только активируется и/или персонализируется, но и создается уже после персонализации карты.

4. Жизненный цикл карты

До того, как карта получает «путевку в жизнь» и выдается владельцу, она последовательно проходит три стадии:

- Изготовление микросхемы;
- Изготовление карты;
- Персонализация карты.

На этапе изготовления микросхемы с микропроцессором производятся следующие основные действия:

- Прожигание (hard-coding) в ПЗУ (ROM) микропроцессора операционной системы чипа (маски).
- Генерация номера микропроцессора и его запись в микросхему.
- Генерация секретного ключа K(IC) (диверсификация от материнского ключа M(IC) по номеру чипа) для микропроцессора и его сохранение в чипе.
- Ключ K(IC) используется для закрытия доступа к карте, а также для передачи секретной информации на карту на этапе ее изготовления.

- Материнский ключ передается Производителю карт.

На этапе изготовления самой карты, после имплантации чипа в пластиковую основу, осуществляются следующие процедуры:

- Фабрика, изготавливающая карты, подтверждает знание ключа K(IC), при этом используется стандартная процедура аутентификации, а именно некоторое псевдослучайное число, полученное от карты устройством предперсонализации, шифруется и возвращается карте для проверки.
- Производится инициализация карты (в EEPROM инициируется файловая система – частично на верхнем уровне или полностью, включая карточные приложения).
- Генерируется и записывается на чипе уникальный серийный номер карты.
- Генерируется секретный ключ KDC (диверсификация от материнского ключа KMC по серийному номеру карты) и загружается в чип (иногда в шифрованном виде с использованием ключа K(IC) или аналогичного).
- Ключ KDC используется для закрытия доступа к карте при транспортировке, а также при передаче секретной информации на карту на этапе ее персонализации.
- Материнский ключ передается персонализатору карты.

Необходимо отметить, что приведена общая схема производства карт с микропроцессором с учетом разграничения ответственности за безопасность. Так, в частности, в описанной последовательности имеется по одному транспортному ключу для микросхемы и самой смарт-карты. На самом деле таких ключей может быть несколько – один для аутентификации карты и устройства, второй для шифрования при загрузке секретных параметров (тех же ключей), третий – для форимрования криптографической подписи при выполнении особо важных команд (например, при создании файловаой структуры карты).

Определенные особенности имеются для карт с открытыми и «закрытыми» операционными системами. Так, например, для Java-карт и карт с Multos, Производитель карт обеспечивает загрузку в ROM соответствующих сертифицированных апплетов международных платежных систем.

Наконец, сам процесс создания приложения (реализации требуемой файловой структуры) может происходить при карточном производстве (предперсонализация, с последующей загрузкой данных), так и на этапе собственно персонализации.

Непосредственно персонализация карты

- Персонализатор карты подтверждает знание ключа KDC.
- Производится персонализация карты (в EEPROM создается файловая система, записываются данные, секретные данные записываются с использованием ключа KDC).

5. Подготовка данных

Общепринято подразделять весь процесс персонализации смарт-карт международных платежных систем на два этапа: подготовки данных и

собственно персонализацию, включающую как персонализацию микросхемы, так и традиционную персонализацию обычных магнитных карт.

Основная задача первого этапа состоит в формировании файла данных, который передается на машину персонализации, будь то эмбоссер или конвейерное устройство для последующего выпуска карточки.

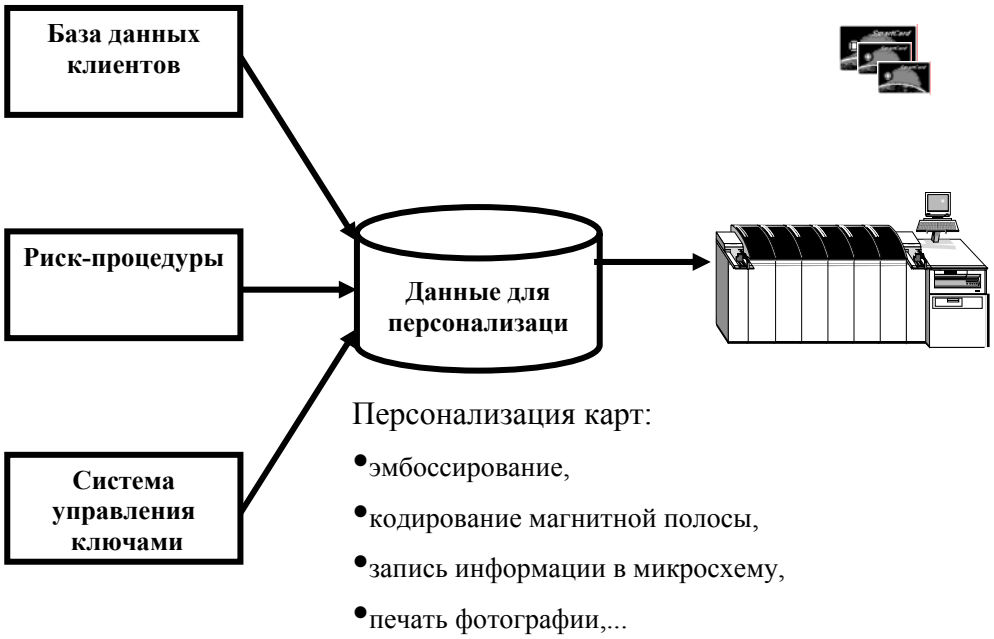


Рис.1. Персонализационные данные

Здесь:

- *База данных клиентов* –это набор данных, относящихся к клиентам – их имена ифамилии (Cardholder Name); сроки действия карточек (Application Effective and Application Expiration Date); номер или PAN (Primary Account Number) и т.д. Все эти данные, как правило, имеются в системе бэк-офиса эмитента традиционных карт с магнитной полосой.
- *Риск-процедуры* – в данном контексте набор параметров, определяющих решения организационного характера, которые принимаются эмитентом и относятся к безопасности функционирования системы и уровню сервиса, предоставляемому клиенту. Здесь имеются в виду методы аутентификации (статическая, динамическая, набор данных для аутентификации), возможность оффлайн-аутентификации, количество попыток для ввода ПИНа, лимиты для оффлайновых транзакций и т.д. При этом, разные клиенты могут по-разному обслуживаться, соответственно и риск-параметры их карточек могут отличаться.
- *Система управления ключами* отвечает за криптографические процедуры, осуществляемые при персонализации карт. Сюда входит список необходимых ключей и областей их применения, методы их генерации, непосредственно генерация и размещение на карте.

Для понимания процесса подготовки данных и далее процесса загрузки данных в микросхему необходимо детально рассмотреть функции, выполняемые основными участниками всего процесса и информационные потоки, возникающие между ними:

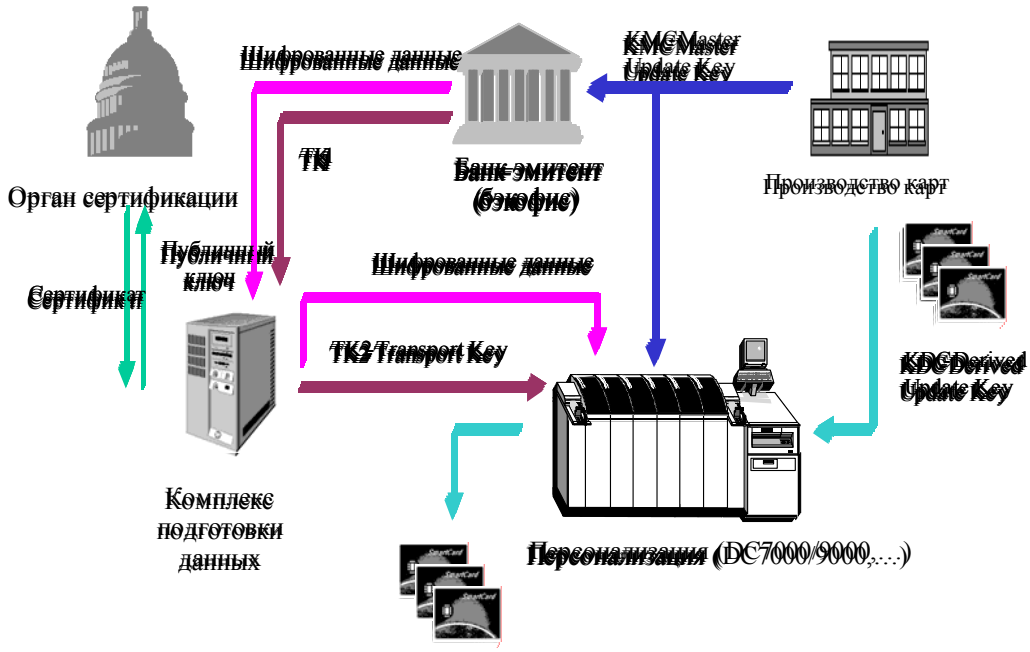


Рис.2. Общая блок-схема процесса персонализации.

В данной схеме, в порядке очередности событий:

- Производитель карт создает KMC – мастер-ключи для доступа к картам в процессе персонализации и переправляет его по секретным каналам Банку-Эмитенту, а также Персонализатору. Способы генерации ключа и его передачи могут быть различными. В дальнейшем Производитель карт «закрывает» доступ к ним с помощью ключей KDC, являющихся производным от KMC. При формировании KDC используется серийный номер карты, что делает каждый ключ уникальным для каждой карточки. Персонализатор, получивший KMC от эмитента, будет «открывать» карточки при помощи ключей KDC, которые будет формировать по тому же алгоритму, по которому это делал Производитель. Алгоритмы шифрования, использующиеся в этих процедурах, как и большинстве других, описываемых дальше – симметричные, как правило, основанные на DES и 3DES, чаще именно один из этих двух. Разумеется, если речь не идет о публичной криптографии, используемой для формирования и проверки сертификатов.
- Производитель карт осуществляет их изгототвление, «закрывает» доступ к ним ключами KDC и отправляет Персонализатору.
- Система бэк-офиса банк-эмитента формирует данные для передачи их в Комплекс подготовки данных (КПД). Часть этих данных являются секретными. К ним безусловно относится PIN, а также могут относиться и другие величины, в зависимости от решений самого банка. Секретные данные шифруются посредством ключа KEK1 (Key Exchange Key 1),

который, в свою очередь, передается в КПД по некоторому секретному каналу.

Среди данных, передаваемых Эмитентом в КПД, находятся также те, которые будут содержаться на поверхности карты (в напечатанном или эмбоссированном виде), а также на магнитной полосе.

- КПД осуществляет генерацию пары несимметричных ключей Эмитента и передает открытые ключи в Орган сертификации платежной системы для создания сертификатов. Орган сертификации подписывает открытый ключ эмитента своим секретным ключом и создает сертификаты, которые будут подтверждать «подлинность» эмитента карты перед терминалом в процессе аутентификации. Помимо открытых ключей Эмитента при создании сертификатов участвуют и другие данные, такие как Issuer Identification Number, Certificate Expiration Date, Certificate Serial Number, Hash Algorithm Indicator. Отметим, что поскольку процесс получения сертификатов достаточно продолжительный, его можно осуществить заранее, еще даже до изготовления карт-заготовок. Сформированный сертификат переправляется в КПД.
- КПД с использованием секретных ключей Эмитента для каждой карты подписывает данные, входящие в список данных статической аутентификации. К ним относятся: Application Effective Date, Application Expiration Date, Application Usage Control, Application Primary Account Number (PAN) и т.д.

  В случае поддержки динамической аутентификации для каждой карты создается своя пара несимметричных ключей, открытый ключ карты подписывается секретным ключом эмитента (аналогично описанной выше процедуре), а секретный ключ загружается на карту для участия в дальнейшем в процессе аутентификации.

  Помимо создания несимметричных ключей эмитента и карт, в стандартные функции КПД входит генерация 3-DES мастер-ключей эмитента и порождаемых ими карточных ключей. К этим ключам относятся:

  А) авторизационные ключи, используемые при генерации и проверке криптограмм,

  Б) ключи, подписывающие скрипты, изменяющие параметры карты,

  В) ключи, шифрующие новые значения PIN.

  Помимо генерации всех необходимых секретных величин, КПД полностью формирует файл с EMV-данными для персонализационного устройства. Секретные данные, в том числе и те, которые были зашифрованы ключом KEK1, «перешифровываются» ключом (набором ключей) KEK2. Полученный файл отправляется Персонализатору. По секретному каналу туда же переправляется ключ KEK2.
- На персонализационном оборудовании «встречаются» карточки, закрытые KDC, и данные, зашифрованные KEK2. Внутри используемого на этом этапе защищенного криптографического устройства, производится расшифровка данных с помощью полученного KEK2. Аналогично, из полученного от Эмитента ключа KMC формируются ключи KDC, с помощью которых «открываются» карты и «перешифровываются» данные для микросхемы. Происходит «внешняя» и «электрическая» персонализация.

Стоит отметить, что в приведенной схеме, как это часто бывает, некоторые из участников могут представлять одно и то же юридическое лицо. Стандартной является ситуация, когда персонализационное оборудование и комплекс подготовки данных принадлежат Эмитенту и располагаются на территории Банка. В то же время, технологически все они являются разными участниками процесса.

Итак, подготовка данных - это ключевой, как в прямом, так и переносном смысле, этап персонализации смарт-карт. За его выполнение ответственность несет программно-аппаратный комплекс, в состав которого входит криптографическое устройство. Рассмотрим более подробно возможную (а зачастую, и требуемую!) его функциональность.

На первом этапе в КПД поступают данные для выпуска карт с магнитной полосой, в том числе информация о владельцах карт. Кроме того, из ограна сертификации платежной системы (Visa, MasterCard) поступает сертификат открытого ключа Банка-эмитента, подписанный открытым ключом платежной системы. Перед формированием SDA к сертификату добавляются также необходимые параметры приложения и эмитента. Вычисление цифровой подписи SDA производится с применением открытого ключа Эмитента. Далее, путем диверсификации симметричного мастер-ключа эмитента (набора ключей) КПД формирует симметричные ключи карты. Затем, если предусмотрена схема DDA, формируются несимметричные ключи карты и вычисляется сертификат публичного ключа (для каждой карты). После добавления параметров, специфичных для карты, а также риск-параметров, задаваемых эмитентом, данные форматируются и готовы к персонализации на устройстве.

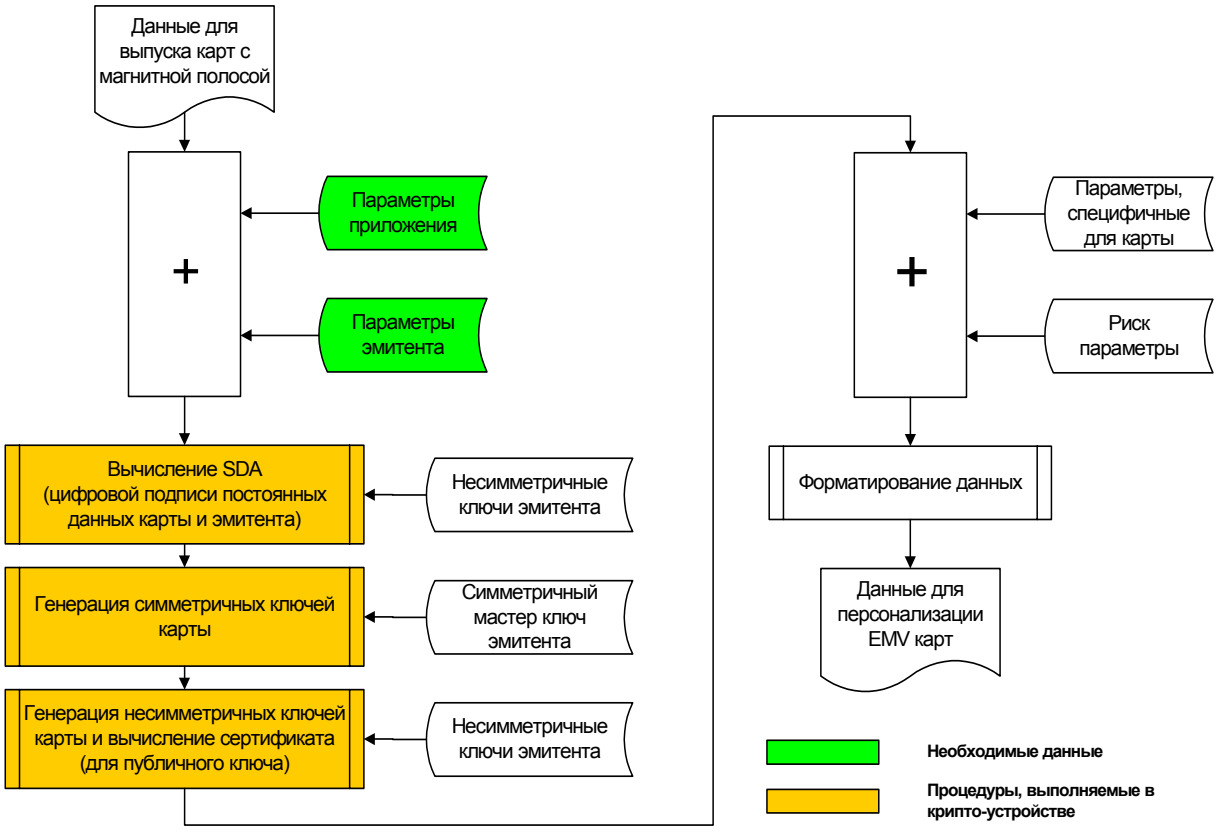


Рис.2. Схема работы КПД

Функциональные возможности КПД:

В процессе своей работы Комплекс подготовки данных оперирует следующими объектами:

- Шаблоны приложений EMV. Включают в себя даные необходимые для персонализации приложения, группировку этих данных по файлам и записям, наборы данных для вычисления сертификатов SDA и DDA, используемые криптографические данные и способы их получения.
- Постоянные значения для ряда используемых параметров. К таким значениям относятся, например, BIN банка, код страны, код валют.
- Шаблоны персонализируемой карты. Включают в себя шаблоны используемых приложений, а также группы постоянных значений, используемые каждым приложением.
- Задание на подготовку данных. Включает в себя используемые шаблоны карт, используемый скрипт ввода данных, список операторов, допущенных к запуску данного задания.

КПД проверяет обрабатываемые данные на правильность формата и допустимых значений (например, месяц в дате не может быть больше 12, а день не может быть больше 31).

Следующие функциональные возможности программного обеспечения являются особенностью «полновесного» Комплекса подготовки данных:

- Взаимодействие с любой системой «Back Office»;
- Поддержка широкой номенклатуры криптоустройств, используемых для генерации криптографических данных;
- Гибкое перераспределение функций по подготовке данных между системой «Back Office» и КПД.
- Поддержка нескольких источников информации для генерации персонализационных данных. Это особенно актуально для выпуска многофункциональных смарт-карт, когда имеется не одно приложние, и информация может приходить из разных источников.
- Поддержка открытых Visa и EMV Common Personalization форматов, которые, как ожидается, в недалеком будущем станут стандартными для всех персонализационных систем.

6. Средства производства

Российская специфика эмиссии карт такова, что большинство банков предпочитает приобретать персонализационное оборудование для того, чтобы выпускать карты, практически не прибегая к посторонней помощи. Основным мотивом такого поведения является естественное нежелание банков предоставлять конфиденциальную информацию о клиентах сторонним компаниям – персонализацинным бюро.

Таким образом, одним из важнейших вопросов является вопрос рационального выбора персонализационного оборудования. Ниже предлагается краткий обзор наиболее распространенных типов устройств самой различной производительности (для персонализационныз бюро и крупных банков, для средних и мелких банков и филиальной сети) и некоторые их характеристики.

Мировым лидером по производству устройств персонализации карт является американская компания DataCard (порядка 85% мирового рынка). Оборудование, выпущенное этой компанией, преобладет в банках большинства стран. Россия не является в этом смысле исключением, более того практически все EMV-карты у нас персонализируются на оборудовании DataCard (не менее 98%).

Свой обзор мы сделаем на примере оборудования именно этой компании, выделив, два типа устройств – настольные эмбоссеры и высокопроизводительные конвейерные комплексы.

Эмбоссеры

Настольные эмбоссеры производства компании Datacard производятся в настоящее время в трех моделях – DC150i, DC280P, DC450. Здесь они перечислены в порядке возрастания производительности. Все устройства могут применяться для персонализации микропроцессорных карт. Для этого на них устанавливаются опциональные модули с встроенным устройством чтения/записи микросхемы. В случае, если эмбоссеры были ранее приобретены без намерения выпускать микропроцессорные карты, данные модули могут быть установлены дополнительно. Реальная производительность самого мощного из эмбоссеров DC450 на международных картах с магнитной полосой может достигать до 300 карт в час (что составляет примерно 12 сек на карту). В то же время DC-150i в состоянии в час персонализировать только около сотни таких карт.

Что же происходит с производительностью эмбоссеров с случае выпуска карт с микросхемой? По нашему опыту для персонализации только одного приложения EMV в самом лучшем случае (для криптографии используется HSM, достаточно «быстрая» карта, не очень сложное приложение) требуется не менее 6-7 сек. В других случаях даже для персонализации только одного приложения это время может возрасти до 15 сек. Следовательно, в час можно выпустить только 120 –180 карт при использовании DC-450 и не более 70 карт на DC-150i.

При персонализации микросхемных карт на настольных эмбоссерах возникают две основные проблемы. Первая состоит в необходимости контролировать процесс выполнения работы на всех этапах перемещения карты от модуля к модулю с целью реагировать на нештатные ошибочные ситуации так, чтобы обеспечить выпуск карт с непротиворечивой информацией (помещаемой на разных модулях – эмбоссирования, кодирования полосы, записи данных в микросхему) и иметь протокол работы о том, какие карты были успешно выпущены, а какие нет. Вторая задача – построение такой технологии, которая позволяла бы гибко управлять именно персонализацией микросхемы, поскольку сам этот процесс (в отличие от стандартизованных процессов для других видов персонализации) достаточно произволен и зависит как от используемых чипов, так и от помещаемых на них приложений.

Таким образом, для управления процессом персонализации на эмбоссере целесообразно использовать специальное программное обеспечение (ПО).

Такое ПО, с нашей точки зрения, должно быть предназначено для решения широкого спектра задач, связанных с разработкой дизайна (определение набора полей персонализации и их параметров), определением информационно-логических связей для полей, описанных в дизайне, а также

непосредственно с изготовлением пластиковых карт, то есть выполнять и роль контроллера эмбоссера.

ПО преобразует формат данных, содержащихся в исходном файле или базе данных, в формат, необходимый для устройства. При этом данные могут быть самого различного характера – от графических изображений до данных, предназначенных для записи в микросхему. При инициализации микросхемы обеспечивается интерфейс к библиотеке прикладных программ (DLL) или программе (COM – объект). В дальнейшем будем назывить прикладную программную компоненту загрузки данных в микросхему ScApp – Smart Card Application. С помощью данного интерфейса обеспечивается обмен данными между ПО - контроллером эмбоссера и ScApp, обрабатываются события, возникающие при персонализации микросхемы.

Ниже на рисунке представлена возможная схема решения задачи персонализации карты на настольном эмбоссере.

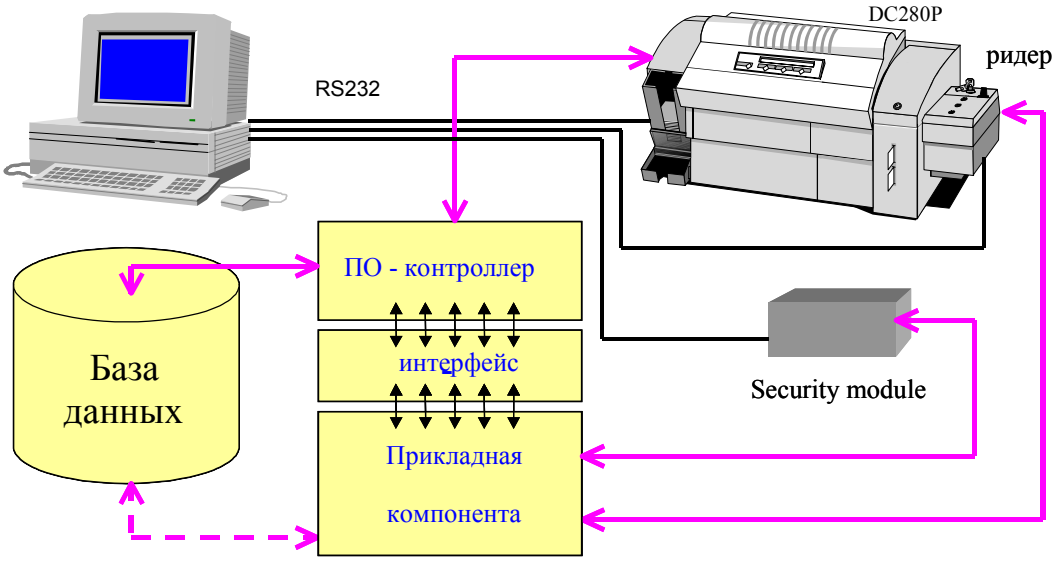


Рис 1. Схема персонализации на эмбоссере.

Конвейерные устройства персонализации

Из высокопроизводительного персонализационного оборудования производства DataCard наиболее актуальны для российского рынка комплексы DC500, DC7000, DC9000. Все они применяютсся и для персонализации смарт-карт.

Функциональне модули этих комплексов (например, модули магнитной записи, графической печати, лазерной гравировки, эмбоссирования) последовательно стыкуются друг с другом, образуя конвейер. При этом происходит параллельная работа модулей, то есть в каждый момент времени персонализируется несколько карт. Именно за счет этого и обеспечивается высочайшая производительность. В то же время контроллер машины обеспечивает информационную синхронизацию выпускаемых карт.

В состав DC500 может входить смарт-модуль с тремя станциями инициализации микросхемы. Производительность устройства принудительно ограничена 500 картами в час.

На комплексах же DC7000 и DC9000 может быть установлено до двух модулей персонализации смарт-карт, каждый из которых содержит до семи станциий инициализации микросхемы или до шести таких станций и станцию маркировки отбракованных карт. Между собой комплексы отличаются возможным количеством устанавливаемых функциональных модулей. Для DC 7000 это количество не превышает шести, для DC 9000 – 20.

Производительность комплекса определяется работой самого медленного модуля в его составе. Обычно таковым является модуль печати цветного изображения (300-500 карт в час). Производительность комплексов при эмбоссировании карт – 500-700 карт в час. В то же время при графической печати и лазерной гравировке в час можно выпускать 1000 и более карт.

Отметим, что для выпуска эмбоссируемых смарт-карт (таких как карты международных платежных систем) с одним EMV-приложением вполне достаточно 3-4 станций программирования.

Работой устройства управляет входящий в его состав специализированный компьютер – контроллер устройства персонализации, обеспечивающий выполнение следующих функций:

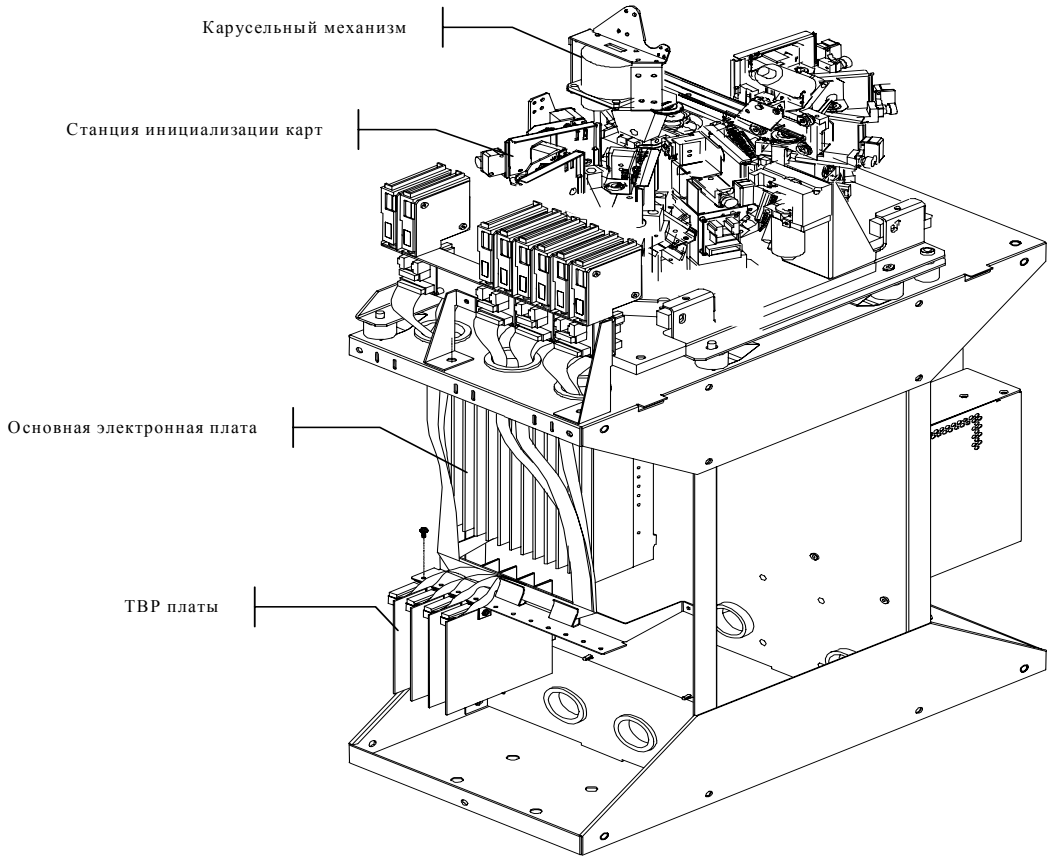
- создание и редактирования наборов параметров, определяющих выполнение процедур ввода данных и процедур персонализации карт;
- ввод и хранение во внутреннем формате потока данных, предназначенных для персонализации пакета карт;
- управление процессом персонализации пакета карт;
- тестирование и настройка параметров работы модулей персонализации карт.

Контроллер функционирует под управлением операционной системы OS/2.

Модуль электрической инициализации микросхем карт (Smart модуль) состоит из:

- карусельного устройства, обеспечивающего механическую подачу карт в несколько станций инициализации,
- станций инициализации карт, каждая из которых оборудована разъемом для подключения к микросхеме карты и соединена с электронной платой, управляющей инициализацией микросхемы (плата ТВР);
- станций шифрования, в которые могут быть помещены SAM-карты, используемые при персонализации и выполняющие определенные криптографические процедуры; каждая из из этих станций соответствует станции инициализации и также подсоединена плате ТВР, кроме того у модуля может быть до 4 общих станций шифрования;
- собственоо плат ТВР управления инициализацией микросхемы;
- основной электронной платы, выполняющей функции управления механизмами модуля, взаимодействия с другими модулями комплекса и передачи данных между контроллером комплекса и платами ТВР.

Ниже на рисунке представлено изображение модуля электрической персонализации микросхемы.



Для повышения быстродействия устройства персонализации в целом Smart модуль позволяет одновременно выполнять электрическую инициализацию нескольких карт по количеству станций инициализации и плат ТВР.

Для управления процессом инициализации микросхемы карты, установленной в станцию, в плату ТВР загружается программа – драйвер ТВР.

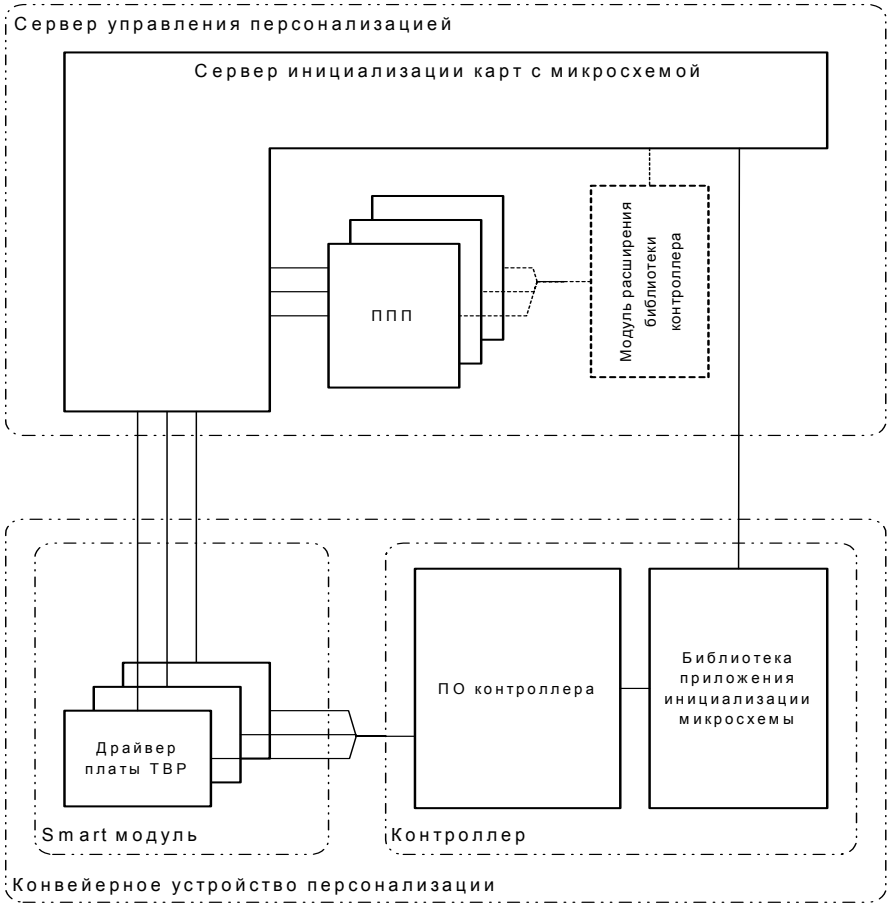
Нужно отметить, что задача персонализации микропроцессорных карт на порядок сложнее, нежели аналогичная для карт с магнитной полосой. Особенно трудной она становится применительно к персонализации на конвейерных устройствах. Причин для этого несколько. Среди них:

- Сложность разработки программных компонент (среда OS/2 и среда кросс-компилятора Franklin для однокристальной ЭВМ Intel 8051).
- Трудоемкость отладки - необходимость использования специальной аппаратуры. Большая доля отладки должна происходить непосредственно на комплексе.
- Уникальность прикладных программных компонент для данного оборудования.

6. Технология промышленной персонализации

В настоящее время разработана технология СПСК (Сервер персонализации смарт карт) для управления процессом персонализаци карт на конвейерных устройствах, а также на эмбоссерах. Технология позволяет персонализировать карты на нескольких, в том числе разнотипных устройствах одновременно. Она настолько универсальна, что при переходе от одних карт к другим, а также от одного типа оборудования к другому, требуется только

изменение модуля ScApp (Программы персонализации приложения), отвечающего за инициализацию конкретного приложения на конкретной карте. При этом, при разработке SCAPP можно ничего не знать об устройстве, на котором будет происходить персонализация.
Ниже на рисунке представлена диаграмма, иллюстрирующая состав и взаимодействие программных модулей СПСК при работе с конвейерным устройством.



В этой схеме:

1. **ПО Контроллера**

ПО Контроллера устройства персонализации обеспечивает управление устройством во время персонализации. Перед началом персонализации пакета карт оно осуществляет действия, необходимые для инициализации аппаратных модулей комплекса. Также под управлением ПО Контроллера выполняется загрузка и инициализация Библиотеки приложения инициализации микросхемы и Драйверов платы ТВР в платы ТВР Smart модуля.

После выполнения процедур инициализации ПО контроллера начинает осуществлять персонализацию карт для текущего пакета данных. Для каждой записи пакета данных, содержащей информацию, необходимую для персонализации одной карты, ПО Контроллера выделяет поля, каждое из которых содержит данные, предназначенные для определенного аппаратного модуля персонализации.

ПО Контроллера взаимодействует с Библиотекой приложения инициализации микросхемы, передавая в нее данные, предназначеные для

персонализации текущей карты пакета. Это производится для того, чтобы предоставить возможность разработчикам приложения инициализации микросхемы карты осуществить обработку данных непосредственно перед процедурой инициализации микросхемы. Примером такой обработки данных могут служить процедуры декодирования зашифрованой информации.

После «предперсонализационной» обработки данных в Библиотеке, ПО Контроллера передает поля данных в аппаратные модули персонализации карты. Данные из поля, содержащего информацию для инициализации микросхемы, передаются в Smart модуль и попадают в ту плату TBP (вернее в загруженный в нее Драйвер), которая соединена со станцией инициализации микросхемы, в которую будет вставлена соответствующая карта.

После завершения процедуры персонализации в каждом модуле устройства в ПО Контроллера передается статус завершения операции. Статус завершения процедуры инициализации микросхемы передается в ПО Контроллера из соответствующего Драйвера платы TBP.

На основании статуса завершения, полученного от аппаратного модуля, ПО Контроллера либо передает в следующий модуль команду на персонализацию карты и соответсующие этой карте данные, либо команду на транспортировку карты через модуль без персонализации в случае ошибки на предыдущем этапе. В зависимости от того, была ли персонализация карты успешной во всех модулях или нет, ПО Контроллера управляет помещением карты в выходной лоток готовых карт или в выходной лоток бракованных карт.

ПО Контроллера учитывает факты успешной или неуспешной персонализации карт и присваевает соответсвующим записям пакета данных соответствующие статусы.

ПО Контроллера является универсальным программным модулем. Оно обеспечивает выпуск различных типов карт, требующих различных способов персонализации за счет создания наборов параметров, описывающих требуемые режимы работы устройства, форматы данных и т.д.

2. **Библиотека приложения инициализации микросхемы**

Библиотека приложения инициализации микросхемы обеспечивает взаимодействие между ПО Контроллера и Сервером инициализации микросхем.

В момент инициализации Устройства персонализации перед началом персонализации пакета карт Библиотека устанавливает соединение с Сервером и передает в Сервер идентификатор типа пакета. По полученному идентификатору Сервер выбирает соответсвующий набор параметров (Задание) для управления инициализацией микросхем карт данного пакета.

В зависимости от особенностей технологии инициализации микросхем данного типа карт и карточного приложения, Библиотека по команде от Сервера может запросить у оператора Контроллера ввести необходимые данные для начала процесса персонализации. Такими данными может быть, например, пароль, необходимый для инициализации миросхем карт данного типа.

В ходе персонализации карт Библиотека принимает от Контроллера данные для персонализации очередной карты перед тем, как они поступят в аппаратные модули Устройства. Она передает эти данные на Сервер для возможной «предперсонализационной» обработки. Примером такой обработки, как указывалось выше, может быть раскодирование зашифрованных данных.

Кроме предварительной обработки данных персонализации, Библиотека получает через ПО Контроллера данные от Драйвера платы TBP с информацией

о завершении процедуры инициализации микросхемы. Эти данные Библиотека также передает на Сервер для возможной обработки, результат которой она возвращает в ПО Контроллера для помещения в журнал выполненых операций.

3. **Драйвер платы ТВР**

Драйвер платы ТВР осуществляет управление платой ТВР для электрической инициализации микросхемы карты.

Он взаимодействует с ПО Контроллера для получения данных для инициализации карты. Полученные данные Драйвер передает в Сервер персонализации. От Сервера персонализации Драйвер получает команды чтения и записи данных в микросхему карты. Последовательность этих команд определяется Модулем инициализации микросхемы, работающем в Сервере. После окончания процедуры инициализации карты Сервер передает в Драйвер информацию о статусе завершения процедуры и сопроводительные данные. Драйвер передает статус и данные в ПО Контроллера.

Программа драйвера реализует различные протоколы, реализующие команды чтения/записи данных в микросхему для взаимодействия с различными типами микросхем карт.

4**. Сервер инициализации микросхем**

Сервер инициализации микросхем выполняет управление програмными модулями, реализующими различные приложения инциализации микросхем для карт различных типов, а также обеспечивает взаимодействие этих модулей с программными модулями, работающими в Устройстве персонализации карт.

Сервер обеспечивает управление произвольным количеством персонализационных устройств с произвольным количеством станций инициализации микросхемы в каждом устройстве.

Сервер поддерживает установку соединения с Библиотекой приложения инициализации микросхемы, получает от нее идентификатор типа пакета персонализируемых карт. По этому идентификатору Сервер выбирает соответствующий набор конфигурационных параметров, называемый Заданием.

Задание содержит в себе следующие описания:

- на каком Устройстве будет выполнятся персонализация карт,
- какие Модули инициализации микросхемы необходимо использовать,
- нужно ли, и если да, то какой Модуль расширения библиотеки контроллера необходимо использовать для данного задания,
- параметры работы приложения при инициализации микросхемы.

После идентификации Задания Сервер выполняет загрузку и инициализацию соответствующих програмных модулей.

Далее сервер обеспечивает взаимодействие этих модулей друг с другом и с программными модулями, работающими в Устройстве персонализации.

Для Модуля расширения библиотеки контроллера Сервер предоставляет механизмы получения и передачи данных в/из Библиотеки приложения инициализации микросхемы в ходе выполнения процедур инициализации, для обработки данных перед персонализацией карты и для обработки данных перед помещением их в журнал операций Контроллера персонализации. Кроме этого Сервер предоставляет Модулю механизмы для передачи данных в Модуль инициализации микросхемы. Как правило этими данными являются параметры,

вводимые оператором Контроллера в момент инициализации. Примером может быть пароль для инициализации микросхемы.

Для каждого Модуля инициализации микросхемы Сервер обеспечивает взаимодействие между Модулем и Драйвером платы ТВР. Кроме этого Сервер предоставляет Модулю механизмы получения данных, переданных от Модуля расширения библиотеки контроллер.

Для всех программных модулей, работающих в его среде, Сервер предоставляет механизмы чтения конфигурационных параметров, а также механизмы протоколирования и трассировки событий, происходящих при работе модулей.

Сервер инициализации микросхем является универсальным программным модулем. Он обеспечивает управление процедурами инициализации микросхем различными Модулями инициализации микросхемы и Модулями расширения библиотеки контроллера, реализующими различные технологии персонализации приложений на микросхемах карт различных типов.

5. **Программа персонализации приложения**

Программа персонализации приложения (Smart Card Application, SCApp) реализует в себе операции, необходимые для инциализации на конкретном типе микросхемы карты приложения или набора приложений конкретного типа.

Программа персонализации приложения работает в среде, создаваемой Сервером инициализации микросхем. Эта среда называется Контекстом. Контекст предоставляет Модулю программные интерфейсы, реализующие следующие функции:

- управление устройством персонализации микросхемы на уровне команд APDU протокола ISO 7816,
- получение данных от ПО контроллера и библиотеки расширения (см. ниже),
- протоколирование событий, происходящих при персонализации микросхемы.

Контекст взаимодействует с Драйвером платы ТВР и, при получении от него данных для инициализации очередной карты, вызывает соответствующие функции модуля, передавая ScApp полученные от Драйвера платы ТВР данные. После завершения процедуры инициализации микросхемы ScApp возвращает в Контекст статус выполнения операции и сопроводительную информацию. Контекст передает эти данные в Драйвер платы ТВР.

Программа персонализации приложения является программным модулем, специфичным для конкретного типа пакета персонализируемых карт.

В настоящее время разработана скрипт-технология, характеризующаяся следующими свойствами:

- Данные для персонализации приложения представлены в виде скрипта;
- Алгоритм персонализации приложений определяется скриптом;
- При переходе к картам другого типа изменяется скрипт, а не программа персонализации приложения;
- Модификация криптографических механизмов не требует модификации программы персонализации приложения.

Таким образом, скрипт-технология позволяет использовать единую SCApp для всех типов карт, эта ScApp представляет собой интепретатор

скриптов, а сами функции загрузки данных в микросхему реализуются скрипт-программами.

6. **Модуль расширения библиотеки контроллера**

Модуль расширения библиотеки контроллера обеспечивает расширение процедур инициализации процесса персонализации карт и процедур обработки данных, специфичное для данного типа приложения, инициализируемого на данном типе карт.

Модуль расширения библиотеки контроллера работает в среде, создаваемой Сервером инициализации микросхем. Эта среда предоставляет Модулю программные интерфейсы, реализующие следующие функции:

- передачу данных в Модули инициализации микросхемы,
- протоколирование событий, происходящих при работе Модуля.

Кроме этого среда Сервера вызывает соответствующие функции Модуля при получении Сервером запросов от Библиотеки приложения инициализации микросхемы. Эти запросы соответствуют следующим действиям:

инциализация процесса персонализации пакета карт в Устройстве; Модуль может в ответ на данный запрос передать в Устройство указание на ввод оператром каких – либо данных;

передача Библиотекой приложения инициализации микросхемы в Сервер данных, введенных оператором;

передача Библиотекой приложения в Сервер данных, предназначенных для персонализации очередной карты для их «предперсонализационной» обработки;

передача Библиотекой приложения в Сервер данных, сопровождающих статус завершения операции инициализации микросхемы, для обработки их перед помещением в журнал Устройства.

Функции Модуля выполняют соответствующую обработку данных и возвращают их в Сервер для передачи в Библиотеку приложения инициализации микросхемы.

Модуль расширения библиотеки контроллера не является обязательным для выполнения процедур инициализации карты. В том случае, если набор параметров Задания Сервера инициализации микросхем не требует использования Модуля расширения библиотеки контроллера, Сервер сам выполняет обработку запросов Библиотеки приложения инициализации микросхемы.

Использование Модуля расширения библиотеки контроллера необходимо в том случае, когда технология инициализации конкретного приложения на конкретном типе микросхемы требует специализированной обработки данных.

Модуль расширения библиотеки контроллера является программным модулем, специфичным для конкретного типа пакета персонализируемых карт.

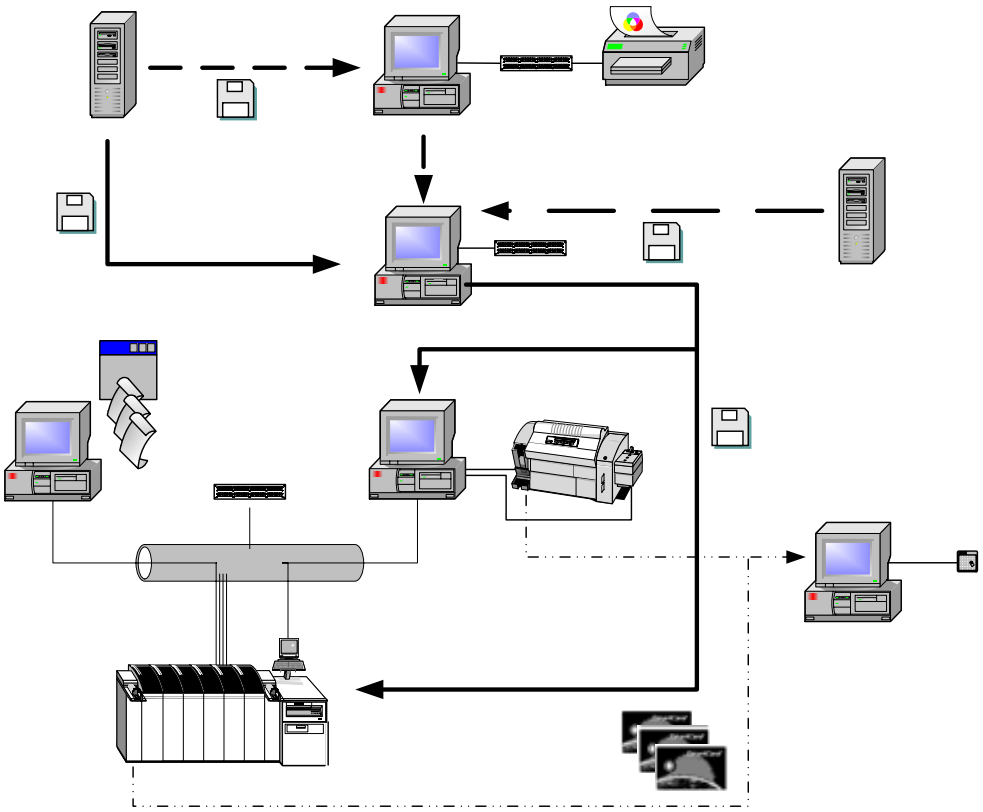
Резюме. Комплексное решение

Из всего вышесказанного следует, что процесс персонализации EMV-карт достаточно сложен, для его решения требуется целый набор организационных, технических , а также программных средств.

В состав комплексного программного решения персонализации входят следующие основные компоненты:

- Система подготовки данных для персонализации (КПД) ,
- Сервер персонализации смарт-карт для управления процессом персонализации микросхем (СПСК),
- Собственно программа персонализации приложения, работающая под управлением сервера (ScApp).

Помимо этих программных компонент целесообразно использовать тестер отперсонализированных смарт-карт для проверки записанных в микросхему данных. Таким образом, вот так может выглядеть общая схема персонализационной системы:



Данные дл
(оп

Система бэк-офиса