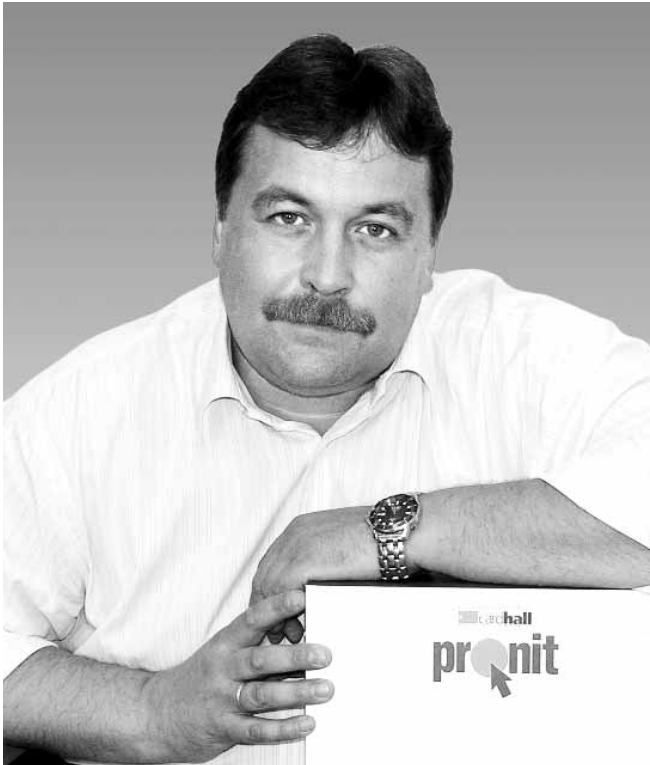


Программное обеспечение для выпуска банковских карт: требования на современном этапе

Дмитрий Сахаров, технический директор ЗАО «ПРОНИТ», группа компаний КАРТХОЛЛ



В последнее время в силу целого ряда различных причин, рассмотрение которых выходит за рамки настоящей статьи, мы наблюдаем устойчивую тенденцию динамичного развития рынка платежных карт, характеризующегося как ростом количественных показателей (объемов эмиссии, количества транзакций, оборотов и т. д.), так и общим повышением активности его участников по всему миру, включая, конечно же, и Россию. Одновременно с этими, безусловно, приятными для большинства читателей журнала «ПЛАС» фактами нельзя оставлять без внимания те проблемы и задачи, которые являются «оборотной стороной медали» роста карточного бизнеса. Таких моментов немало, причем с развитием рынка их перечень постоянно расширяется, и сегодня уже не представляется возможным хотя бы в двух словах обсудить все «узкие места» в рамках одной публикации или доклада того или иного специалиста. Поэтому в этот раз мы постараемся рассмотреть ту часть насущных вопросов, которые связаны с выпуском и персонализацией пластиковых карт, а также кратко коснуться особенностей программных продуктов компании ПРОНИТ (группа компаний КАРТХОЛЛ), которые обеспечивают их эффективное решение.

Большинство программных продуктов компании ПРОНИТ успешно зарекомендовали себя на рынке в течение ряда последних лет. Среди них можно выделить следующие решения:

- DeskPerso – управление персонализацией пластиковых карт в настольных устройствах;
- MSDP Manager – генерация данных для карт с магнитной полосой и печать ПИН-конвертов;
- SmartDataCenter – подготовка данных для персонализации приложений микропроцессорных карт;

- SCPE – управление персонализацией микропроцессорных карт;

- KeyCompass – управление криптографическим оборудованием SafeNet (Eradicom), Thales e-Security и SAM-картами;

- EMV Insight – тестирование EMV-карт.

Наряду с этими продуктами в 2007–2008 годах компания ПРОНИТ разработала и внедрила в ряде банков систему Ostorus*, которая предназначена для автоматизации технологических процессов персонализационного бюро.

Итак, рассмотрим функциональные возможности данных решений компании

сквозь призму основных проблем обеспечения безопасности при выпуске пластиковых карт, моментов, связанных с влиянием «человеческого фактора», а также проанализируем последние достижения и инновации компании ПРОНИТ в данной области.

Безопасность превыше всего

Как гласит известный закон, если в окружающем нас мире какое-либо явление демонстрирует рост, то при этом возрастают (как минимум в абсолютных, а то и в относительных величинах) не только

*Подробнее о системе Ostorus читайте в материале «Управляемость и информационная безопасность персонализации», «ПЛАС» №8 –9/2006

для выпуска карт и заканчивая процедурами утилизации бракованных карт и карт, срок действия которых истек.

Существует ряд дополняющих друг друга технологий, обеспечивающих надежность защиты данных при их передаче между различными участниками процесса генерации персонализационной информации / выпуска карт, а также в период оперативного хранения данных в различных системах, используемых на данных технологических этапах.

Одним из основополагающих методов защиты является шифрование персонализационной информации, содержащей в себе секретные величины: проверочные значения для магнитных дорожек, проверочные значения для ПИН-кода и т. д. Стандарт PCI DSS четко определяет, что «шифрование является фундаментальным компонентом защиты данных держателя карты. Так, если преступник преодолевает сетевые средства защиты и получит доступ к зашифрованным данным, не обладая соответствующими криптографическими ключами, эти данные останутся нечитаемыми и, соответственно, бесполезными для него».

Для обеспечения соответствия своих решений стандарту PCI DSS компания ПРОНИТ внесла в них ряд модификаций. Теперь пользователи систем MSDP Manager (генерация данных для магнитной полосы, генерация ПИН-кода и печать ПИН-конвертов) и SmartDataCenter (генерация EMV-данных) могут использовать шифрование для обеспечения безопасности карточных данных. Новая функциональность базируется на модернизации возможностей криптографической подсистемы Key Compass. Ее последние версии позволяют шифровать информационные потоки, обрабатываемые на входе и выходе прикладных систем. Кроме этого, мы начали предоставлять набор средств разработчика (SDK) подсистемы Key Compass для реализации защиты данных на основе шифрования в прикладных системах других компаний.

Такое решение позволяет легко защитить информационные потоки в процедурах удаленного выпуска карт и печати ПИН-конвертов. В ряде банков технология шифрования данных уже применяется в соответствующих промышленных системах (см. рис. 1).

Говоря о вопросах обеспечения безопасности при работе с персонализационными данными, нельзя обойти вниманием такой важный аспект, как контроль и ограничение доступа персонала персонала к информации. Эффективным решением такого рода задач является использование промышленных систем управления базами данных (далее – СУБД) для оперативного хранения информации и ее обработки.

В качестве примера таких систем можно привести хорошо всем известные продукты компаний Oracle и Microsoft, а также ряд других реализаций. За счет встроенных средств ограничения и контроля доступа, а также за счет шифрования хранилища данных эти системы предоставляют эффективные решения для обеспечения безопасности.

В качестве наиболее показательных примеров использования промышленных СУБД можно привести персонализационные системы нового поколения Maxsys, MX6000 и MX2000, а также систему Ostorus, разработанную компанией ПРОНИТ для автоматизации деятельности персонализационных бюро. Система Ostorus, использующая СУБД Oracle, позволяет не только контролировать доступ к данным, расположенным в хранилище системы, но и обеспечивает дополнительные прикладные функции управления и контроля. Одним из примеров реализации такого функционала является специальная конфигурация установки системы, дающая возможность оператору, выполняющему процедуры загрузки данных, видеть списки файлов, но не иметь возможности просматривать информацию, хранящуюся в этих файлах.

Помимо этого, в системе Ostorus прототоколируются все действия персонала, в том числе такие, как вход в систему, завершение работы, изменение настроек, выполнение производственных задач и т. п. Данная функциональность реализована таким образом, что доступ к журналу операций имеют ограниченное количество сотрудников. Это обеспечивает возможность создания отдельной службы, обеспечивающей мониторинг действий персонала (см. рис. 2).

Говоря о вопросах безопасности, необходимо также затронуть ряд вопросов, касающихся соответствия требованиям стандарта PCI DSS и возникающих в организациях, эксплуатирующих конвейерные устройства предыдущего поколения – это широко распространенные на рынке комплексы DC 9000/9000E, DC 7000 и DC 500. Эксплуатация этих машин предполагает оперативное хранение данных в файлах на управляющих компьютерах комплексов в открытом виде. Кроме того, повышенные риски обуславливает использование на управляющем компьютере морально устаревшей операционной системы OS/2 компании IBM, не имеющей встроенных средств ограничения доступа и защиты информации. Управляющие программы персонализационных машин не обеспечивают эффективного учета количества экземпляров карт, выпущенных для одной записи данных.

Для обеспечения защиты по всем перечисленным направлениям компания ПРОНИТ предлагает организациям, использующим машины этого типа, свое решение PersoDataProtector, в рамках которого хранение оперативных данных обеспечивается во внешнем по отношению к персонализационной машине сервере, использующем промышленную СУБД для обеспечения защиты данных и контроля доступа. В управляющую программу персонализационной машины встраивается модуль, который обеспечивает в момент выпуска карты взаимодействие с сервером системы PersoDataPro-

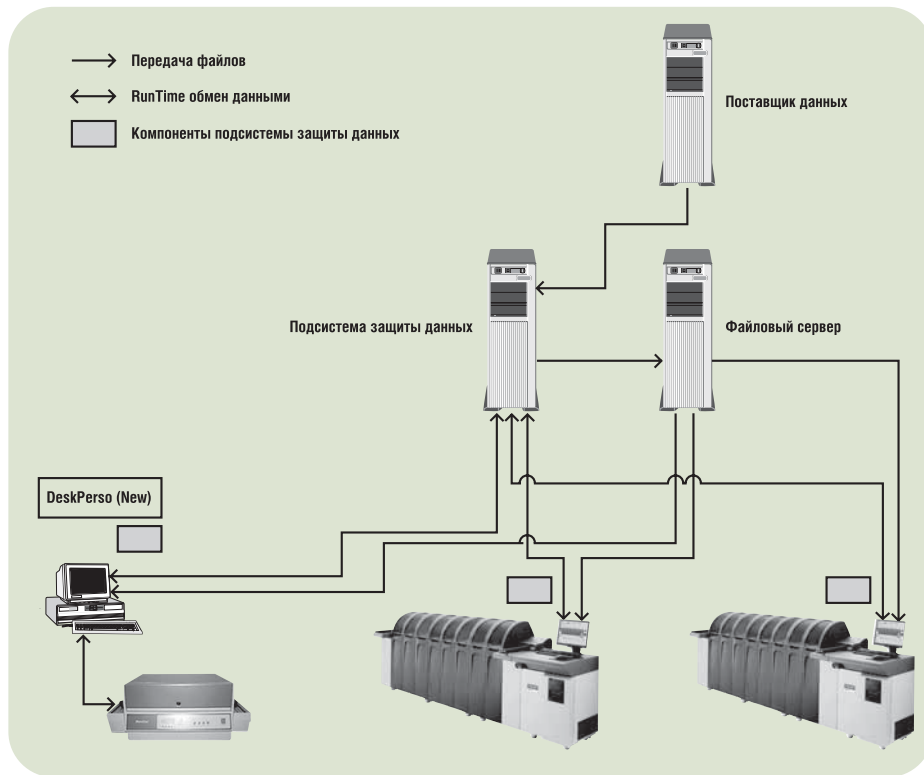


Рис. 3. Структура системы PersoDataProtector

щие под управлением ПО DeskPerso (см. рис. 3).

Таким образом, это решение позволяет предотвратить хранение данных в открытом виде на управляющем компьютере персонализационного устройства, исключить бесконтрольный выпуск карт, а также разграничить действия персонала по выпуску и перевыпуску карт, например, между оператором и начальником смены.

Минимизация негативного влияния человеческого фактора

Говоря о проблемах организаций, занимающихся выпуском платежных карт, необходимо признать, что использование даже самых лучших, самых «правильных», т. е. абсолютно свободных от ошибок программных решений (представим себе, что существует хотя бы одно такое «безошибочное» решение, например, принесенное нам в дар представителями внеземной цивилизации) не может гарантировать отсутствие брака и возникновения различного рода иных «недоразумений» в повседневной деятельности. Причины этого тесно связаны с пресловутым человеческим фактором. Очевидно, что для их решения недостаточно самих по себе возможностей программных систем, обеспечивающих надежность, защищенность, гибкость персобиюро и т. д. Необходимы также различные административные меры, регламентирующие действия персонала. Говоря о человеческом факторе, мы подразумеваем прежде всего ошибки сотрудников, часто возникающие в результате обслуживания большого потока информации, высокой интенсивности работы и целого ряда других причин. С учетом этих реалий компания ПРОНИТ считает одной из своих первоочередных задач построение программных продуктов и технологий таким образом, чтобы минимизировать риск возникновения ошибок, связанных с влиянием человеческого фактора, на всех этапах производства.

Задание на эмбоссирование

Продукт

Дизайн заготовки:

Visa Electron Sport



Наименование задания
 Оператор, создавший задание
 Количество карт
 Job Setup на эмбоссере
 Имя эмбоссера
 Путь к файлу
 Имя файла

06-08-2008 (103)
 Васюткин А.П.
 55
 Visa_Electron
 Комплекс DC7000 700-3701
 V:\EMBS\CARD
 V_EL_SPORT_1135.DAT

Рис. 4. Фрагмент документа «Задание на эмбоссирование»

тестор и получение от него данных, «срок жизни» которых ограничен временем выполнения процедуры персонализации текущей карты. При этом процедура контроля количества экземпляров карт, выпущенных для каждой записи данных,

производится именно на стороне сервера системы, а не на стороне персонализационной машины.

Система поддерживает не только контроллерные устройства персонализации, но и «настольные» машины, работаю-

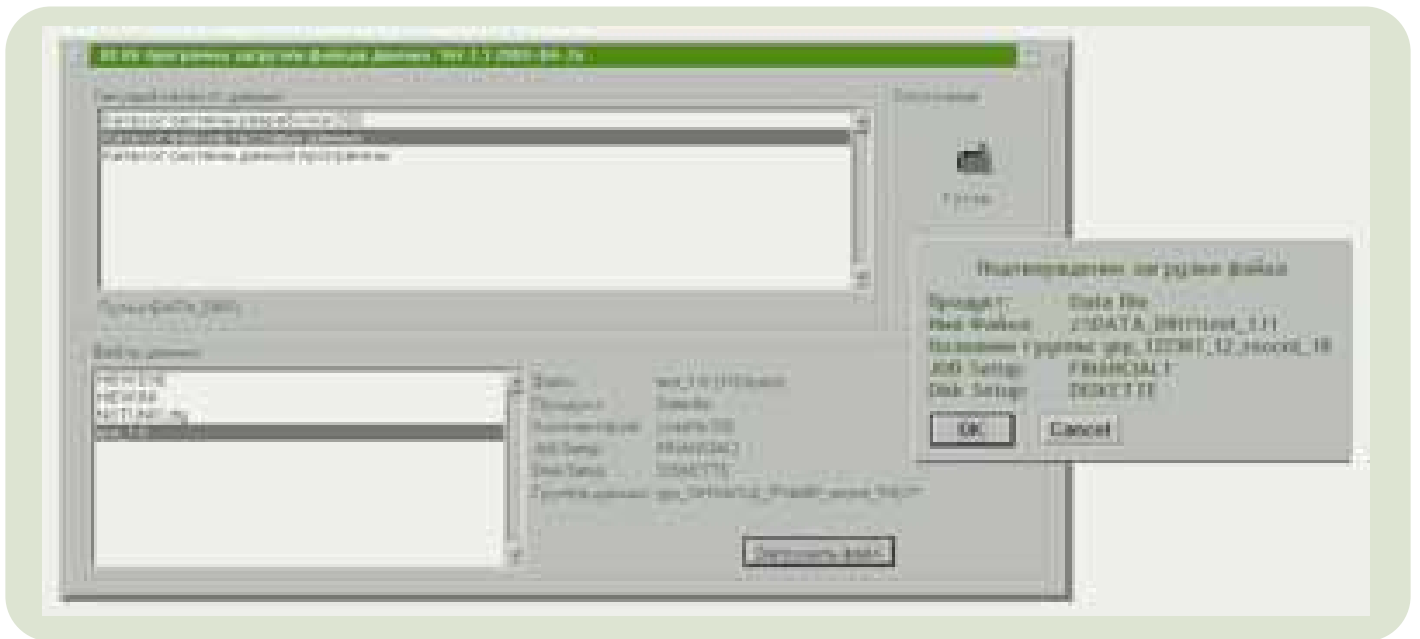


Рис. 7. Распределение партий готовой продукции на партии на отгрузку

Наиболее распространенными, по нашему мнению, являются следующие ошибки:

- ошибки, связанные с использованием некорректного набора настроек устройства при выпуске карт конкретного типа. Классический пример тому – выпуск карт категорий Gold с заданными настройками для выпуска карт категории Classic, что ведет к очевидному браку;
- ошибки, обусловленные внешней схожестью заготовок карт для различных персонализируемых карточных продуктов;
- ошибки, возникающие при появлении карт, которые в силу сбоев оборудования персонализированы частично. Операторы, пытаясь исправить такие карты, путают и смешивают данные. В результате заурядной становится ситуация, при которой на карте с помощью эмбоссирования нанесены номер, имя держателя и дата окончания действия карты, не соответствующие информации, записанной на магнитной полосе.

Для снижения вероятности возникновения описанных выше ситуаций мы предлагаем использовать ряд функциональных возможностей систем разработки компании ПРОНИТ, а также отдельные

утилиты, специально созданные для облегчения работы операторов.

Флагманом среди продуктов ПРОНИТ, предназначенных для эмитентов платежных карт, можно назвать систему Ostorus, являющуюся фундаментом для обеспечения бесперебойного функционирования персобию с большим количеством оборудования и многочисленным персоналом. В качестве примера того, каким образом решается задача сокращения операторских ошибок с помощью Ostorus, можно привести стандартный документ, генерируемый системой – «Задание на эмбоссирование» (см. рис. 4). Он автоматически создается в тот момент, когда оператор формирует файл с данными для персонализационного устройства. В «Задании на эмбоссирование», среди прочего, содержится следующая информация:

- название файла с данными;
- изображение лицевой и оборотной стороны заготовки карты;
- название устройства;
- название набора настроек устройства (Job Setup / Схема связей), которые необходимо использовать.

«Задание на эмбоссирование» позволяет в явном виде – печатном варианте – пе-

редать от руководителя смены оператору указание, какую работу необходимо выполнить. Но вот оператор подошел к персонализационному комплексу, и перед ним стоит задача ввести значения в несколько полей, указывая, какой именно файл и с какими настройками надо обрабатывать. Для того чтобы предотвратить возможные при выполнении этой процедуры ошибки сотрудника и упростить выполняемые им действия при работе на конвейерных машинах предыдущего поколения, мы предлагаем новую утилиту «DCXk Data Loader».

Данная утилита использует простые правила, позволяющие связать имя файла данных с карточным продуктом, а следовательно, и с названием настроек персонализационной машины, напоминая оператору об использовании ленты топирования соответствующего цвета и т. д. Оператор в пользовательском интерфейсе утилиты выбирает файл для выпуска очередной группы карт и нажимает одну-единственную кнопку, давая команду загрузить данные из выбранного файла в управляющую программу персонализационной машины и начать выпуск карт (см. рис. 5).

«DCXk Data Loader» автоматически передает в управляющую программу все не-

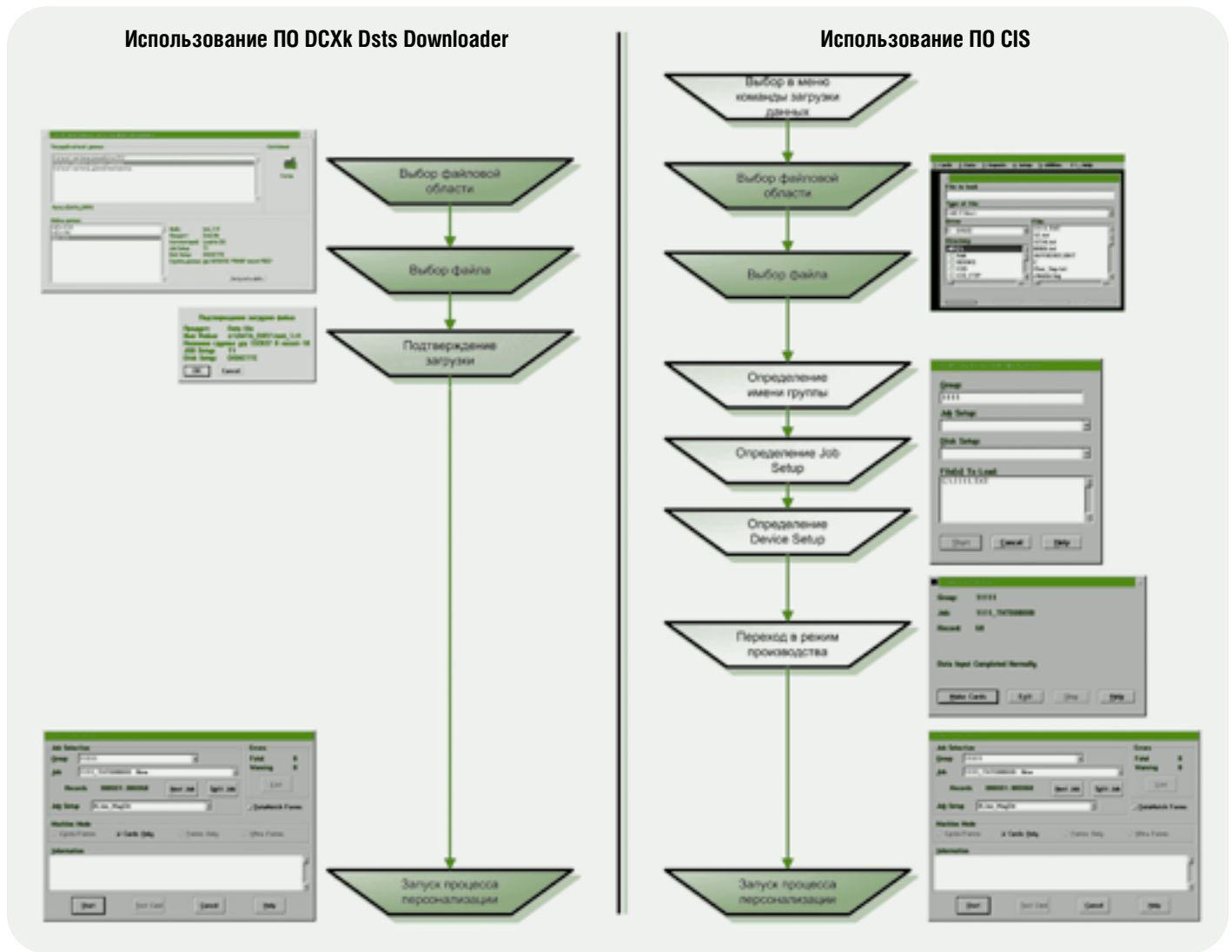


Рис. 6. Сравнение алгоритмов действий оператора персокомплекса

обходимые величины – названия Job Setup, Disk Setup, группы данных и т. д. Таким образом, решаются сразу две задачи, первая из которых – минимизация вероятности ошибки оператора при выборе настроек для выпуска конкретного типа карт, а, вторая – сокращение количества действий оператора, необходимых для начала выполнения задания.

Как демонстрирует диаграмма, приведенная на рис. 6, количество действий оператора, использующего «DCXk Data Loader», сокращается почти вдвое.

Еще одним важным моментом в борьбе за качество работы персобюро является

задача тестирования выпущенных карт, так как помимо очевидного брака существует вероятность возникновения ошибок, которые невозможно проконтролировать визуально: магнитная полоса может оказаться поврежденной, перепрограммированная память микросхемы, возможно, несет в себе сбои, не позволяющие работать EMV-приложению, и т. д. Таким образом, существует большое количество возможностей для возникновения скрытых дефектов персонализации. Для их выявления компания ПРОНИТ предлагает прекрасно зарекомендовавший себя на рынке продукт – систему EMV Insight**.

Это комплексное решение позволяет проконтролировать работоспособность отдельных элементов выпущенной карты, таких как микросхема или магнитная полоса, а также выполнить проверку согласованности данных, нанесенных на поверхность карты, записанных на магнитную полосу и в память микросхемы.

«...по улицам курьеры, курьеры, курьеры...»

Эта знакомая нам с детства фраза из «Ревизора» Гоголя часто вспоминается в тот момент, когда обсуждение касается финального этапа деятельности персонали-

**Подробнее о системе EMV Insight читайте в материале «Контроль качества производства и персонализации карт», «ПЛАС» № 2/2008

зационного подразделения банка. Именно тогда возникает задача сортировки и отправки карт в банковские филиалы и сторонние организации. С этим процессом связано выполнение трудоемких процедур и решение большого количества задач, возникающих при работе службы контроля качества и сортировки готовой продукции:

- формирование партий карт, отсылаемых в банковские филиалы и сторонние организации;
- печать сопроводительных документов;
- контроль наличия всех заказанных карт;
- выявление брака;
- ... и т. д.

Суть процессов, выполняемых на этом этапе, отражена на диаграмме, приведенной на рис. 7:

Для автоматизации процедур сортировки и контроля качества персонализации, а также для учета карт, выпущенных на персонализационном оборудовании, компании ГАММА КАРТ и ПРОНИТ, входящие в группу компаний КАРТХОЛЛ, предлагают программно-аппаратное решение, включающее в себя машину CardsMaster и программное обеспечение Card Inspector.

Машина CardsMaster представляет собой конвейерное устройство, которое способно распределять карты из входного лотка по различным выходным лоткам, причем управляющая программа Card Inspector позволяет делать это на основе либо результатов контроля качества карт, либо конкретных правил, формализованных в задании, выполняемом этой машиной, либо по совокупности двух этих задач. Таким образом, данный программно-аппаратный комплекс может использоваться как для контроля качества выпущенных карт (в том числе данных, записанных на магнитной полосе, информации EMV-приложения и иных характеристик), так и для сортировки карт по различным группам, например, для отправки в различные филиалы банка. Автоматически при этом решается задача проверки наличия в партии всех карт, которые

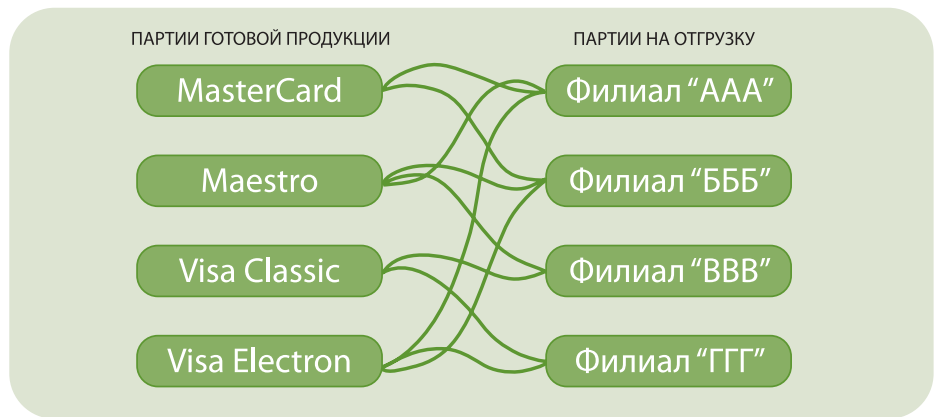


Рис. 7. Распределение партий готовой продукции на партии на отгрузку



Рис. 8. Машина CardsMaster

должны были быть выпущены в рамках конкретного задания или набора заданий.

В настоящий момент в компании ПРОНИТ ведутся работы по интеграции программно-аппаратного комплекса CardsMaster и Card Inspector в систему Ostorus, что позволит сделать процедуры проверки качества карт и их сортировки частью общего технологического процесса, управляемого системой Ostorus.

Процесс сортировки и отправки карт связан с обслуживанием больших объемов документации, сопровождающей продукцию персонализационного бюро при доставке конечному потребителю (филиалу банка, сторонней организации и т. д.). Зачастую подразделения, занимающиеся процедурами сортировки и отправки, и подразделения, занятые непосредственно выпуском карт, являются различными службами внутри одного отдела или управления, поэтому между ними может существовать собственный документообо-

рот. Проблемы, связанные с избыточным документооборотом, минимизируются с помощью системы Ostorus, позволяющей вести учет партий готовой продукции, передаваемых из персобюро в службу доставки и сортировки, обеспечивать подготовку документов для передачи партий продукции на отгрузку в почтовые службы, транспортные компании или непосредственно курьерам для доставки продукции конечному потребителю. Система Ostorus позволяет выпускать широкую номенклатуру производственных аналитических отчетов, причем поддерживает работу как одного персонализационного подразделения банка, так и нескольких персонализационных бюро, функционирующих в различных филиалах банка.

А что там, значительно ближе горизонта?

Традиционно дальнейшее направление развития программных продуктов компа-

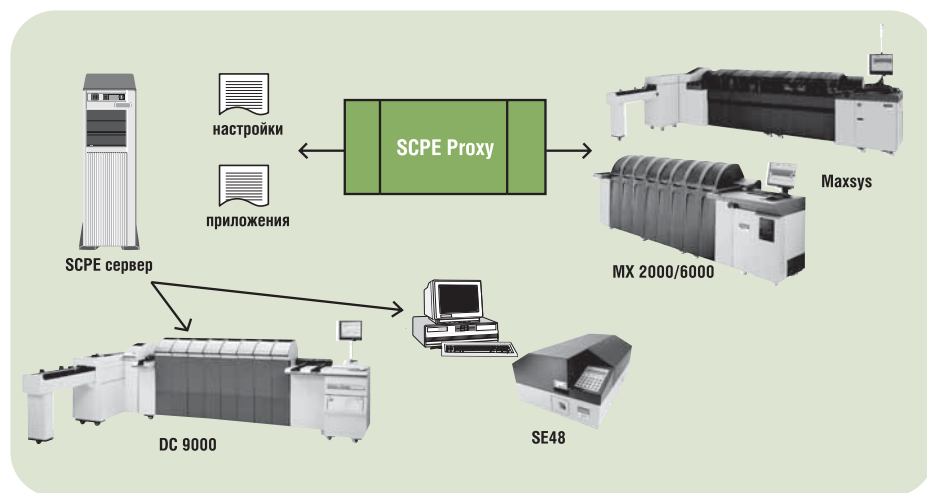


Рис. 9. Модуль SCPE Proxy в персонализационной системе на основе сервера SCPE

нии ПРОНИТ определяют самые разные объективные факторы: это и постоянно обостряющаяся конкурентная борьба банков за потенциального клиента, и как одно из следствий – повышенный интерес эмитентов к выпуску карт с индивидуальным дизайном; выход на рынок новых моделей цифровых фотоаппаратов; совершенствование отраслевых стандартов и спецификаций в индустрии микропроцессорных карт – все эти разнородные события находят отражение в наших решениях.

Мы постоянно модернизируем широко известную и хорошо себя зарекомендовавшую программу DeskPerso, управляющую «настольными» устройствами персонализации. На сегодняшний день DeskPerso обеспечивает работу с такими новыми моделями персонализационного оборудования, как, например, «настольные» эмбоссеры SE48 и принтеры RP90 Plus E, в которых реализована ретрасферная технология печати, что позволяет наносить изображение на карты «из края в край» и выпускать карты с индивидуальным дизайном. В связи с расширением моделей фототехники на современном рынке в последних версиях DeskPerso реализована поддержка линейки фотоаппаратов Cannon Power Shot, что позволило пользователям программного обеспечения использовать это оборудование для получения более

качественных снимков при выпуске карт с фотоизображением.

Происходящая в течение последних двух лет смена линеек конвейерных устройств привела к появлению новых компонент в системах персонализации микропроцессорных карт. Для обеспечения выпуска такого типа карт на новых машинах серии MaxSys, MX 6000 и MX 2000, имеющих в составе программного обеспечения модули Affina производства Datascard, компания ПРОНИТ разработала новую компоненту SCPE Proxy. Эта компонента обеспечивает взаимодействие между упомянутыми выше устройствами и средой персонализации микропроцессорных карт SCPE. SCPE Proxy позволяет интегрировать новые устройства в существующую инфраструктуру, не требуя изменения настроек или приобретения новых реализаций приложений для персонализации карт. Архитектура модуля SCPE Proxy дает возможность управлять персонализацией микропроцессора карты не только в новых конвейерных устройствах, но и расширяет возможности технологии SCPE для поддержки любых персонализационных систем (см. рис. 9).

Еще одним направлением развития технологий и программных продуктов компании ПРОНИТ стала поддержка новых видов микропроцессорных карт, начавших получать широкое распространение на

рынке в 2007–2008 гг. Речь идет о картах Global Platform, удовлетворяющих спецификациям Global Platform версии 2.2.1. Характерной особенностью этих карт является использование новых механизмов при шифровании данных. Современные версии скриптов персонализации и криптоподсистемы обеспечивают поддержку криптографических технологий, что позволяет персонализировать карточные продукты на основе таких карт, как современные Java-карты компании Gemalto, JCOP S10, S20, 21, Kona 20, 25, 23S, 11 и т.д., а также выполнять персонализацию апплета M/Chip4 на картах GXP, GCX и Palmera Air.

Говоря о новых технологиях, нельзя не упомянуть и о применении дополнительного домена безопасности на картах Global Platform с несколькими приложениями. Наличие дополнительного домена безопасности обеспечивает возможность разделения ключей эмитента карты и ключей приложений с удовлетворением всех требований безопасности, которые возникают в любых системах, основанных на мультиаппликационных картах, где эмитентами приложений выступают различные организации и участники. Последние версии продуктов компании ПРОНИТ для подготовки данных и персонализации карт Global Platform поддерживают работу с дополнительным доменом безопасности. Примером является успешный проект с нашим участием, реализованный в Казахстане, в рамках которого на многофункциональных картах с микросхемой размещено приложение «Талон водительского удостоверения».

Поддержка клиентов как гарантия успеха

Компания ПРОНИТ постоянно повышает качество своих продуктов для эмиссии многофункциональных чиповых карт. Наши специалисты поддерживают программные продукты в соответствии с новыми нормативными документами международных платежных систем, а также дополняют их новым функционалом.

Пройдя определенный путь в развитии карточного бизнеса вместе с эмитентами пластиковых карт, специалисты ПРОНИТ имеют четкое представление о том, что успех эксплуатации программных продуктов зависит от качества их поддержки. Под поддержкой ком-

пания понимает не только и не столько решение вопросов, возникающих при эксплуатации программных продуктов, сколько содействие в достижении цели клиентов стабильного выпуска карт, сертифицированных международными платежными системами. Поэтому спе-

циалисты компании оказывают эмитентам реальную помощь в прохождении сертификации. Подтверждение тому – 14 из 15 эмитентов EMV-карт, являющихся клиентами ПРОНИТ, прошли сертификацию в платежных системах с первого раза.

ПЛАС

КАЛЕЙДОСКОП 