

Технология выпуска EMV-карт в присутствии клиента банка

Дмитрий Сахаров, технический директор ЗАО «ПРОНИТ», группа компаний КАРТХОЛЛ,
Юрий Перлин, зам. генерального директора ЗАО «ПРОНИТ», группа компаний КАРТХОЛЛ



Юрий Перлин



Дмитрий Сахаров

I. Предпосылки выпуска карты в присутствии клиента

Как известно, современная ситуация на рынке банковского обслуживания физических лиц характеризуется такими тенденциями, как широкое распространение кредитных карт, острая конкурентная борьба за клиентов, постоянное стремление к снижению себестоимости обслуживания, а также повышение уровня безопасности в различных сферах деятельности, связанных с применением платежных карт при выполнении финансовых операций.

Любой розничный банк, желающий быть конкурентоспособным, а значит – совре-

менным и привлекательным для клиентов, ставит перед собой следующие цели:

- повышение качества обслуживания клиентов на фоне усиливающейся конкурентной борьбы;
- оперативный охват новых географических территорий;
- эффективные маркетинг и брендинг, ориентированные на массовое привлечение новых клиентов.

Одним из шагов на пути к достижению этих целей является, в частности, сокращение времени проведения процедур, связанных с выпуском и выдачей клиенту карточки банка. Так, во многих случа-

ях клиент предпочел бы при визите в банк написать заявление о выдаче карты и сразу же ее получить. Не менее важным фактором является упрощение этих процедур, что позволяет, с одной стороны, снизить их себестоимость, а с другой – повысить их безопасность. Примером такого упрощения может быть отказ от практики выдачи клиенту банка традиционного ПИН-конверта, содержащего его ПИН-код. Вместо этого клиент банка должен иметь возможность определить ПИН-код своей будущей карты в момент написания заявления об открытии карточного счета.

Данные задачи обуславливают необходимость создания технологии и реализующей ее системы, позволяющих выпускать карточки в присутствии клиента банка, минимизируя время, требуемое на оформление договорных отношений между банком и его будущим клиентом, последующую генерацию соответствующих данных во всех системах банка и непосредственно на процедуру изготовления экземпляра платежной карты.

К такой системе предъявляется ряд достаточно разнородных требований. В частности, система должна:

- поддерживать распределенную топологию, обеспечивающую большое количество рабочих мест операторов, территориально удаленных от центрального офиса;
- использовать простое и доступное по цене оборудование на удаленных рабочих местах операторов;
- обеспечивать легкость и оперативность развертывания удаленных рабочих мест операторов;
- функционирование системы должно быть организовано таким образом, чтобы она позволяла выпускать карту, в том числе и EMV, в присутствии клиента;
- удовлетворять существующим требованиям по безопасности и защите данных;
- обеспечивать простые процедуры конфигурации и настройки параметров;
- обеспечивать эффективный мониторинг своей работы.

II. Структура системы

Структура системы, удовлетворяющей вышеперечисленным требованиям, приведена на рис. 1.

Предлагаемая ЗАО «ПРОНИТ» система имеет ядро, размещенное в процессинговом центре банка, где сконцентрированы АБС, система ведения клиентов и система управления карточками. Ядро обслуживает произвольное количество удаленных рабочих мест операторов, которые могут устанавливаться либо в офисах банка, либо вне офисов – в местах большого скопления потенциальных клиентов банка, напри-

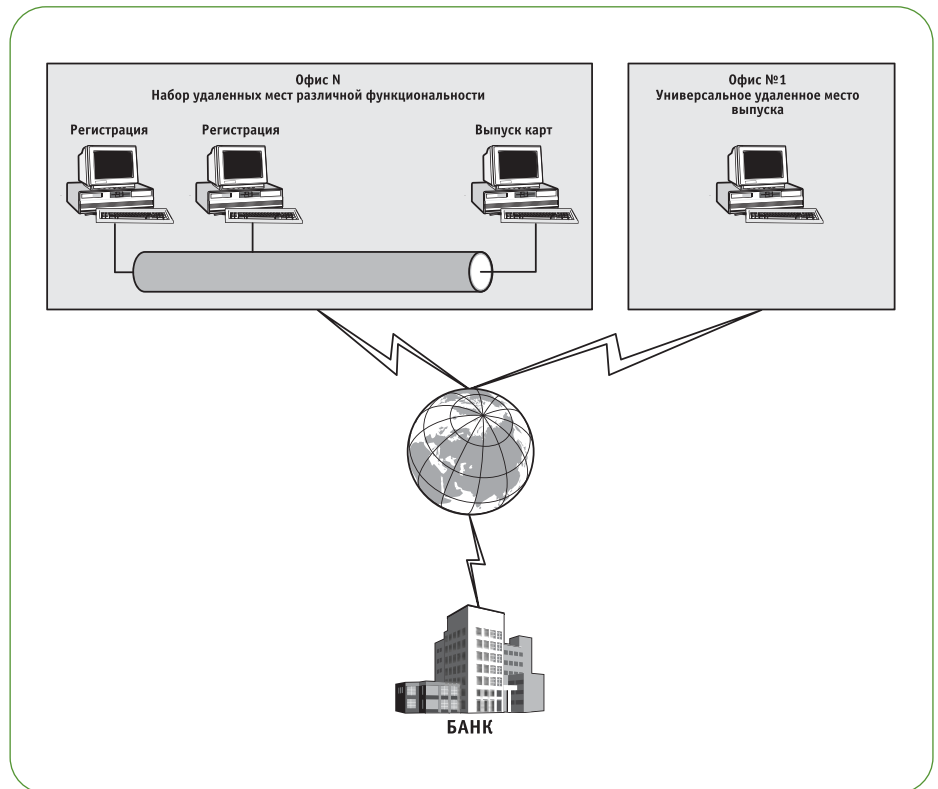


Рис. 1. Структура системы

мер, на крупных спортивных соревнованиях, на выставках, в больших торговых центрах во время проведения рекламных акций, целенаправленно воздействуя на людей и формируя клиентскую базу. В первом случае (рабочее место оператора установлено в офисе банка) функциональность системы может быть разделена между несколькими рабочими местами, каждое из которых реализует некоторое подмножество операций, выполняемых при заключении договора с клиентом и выпуске для него карты. Во втором случае (при мобильном выпуске карты вне офисов банка) удаленное рабочее место должно обеспечивать выполнение всех требуемых операций, т. е. быть универсальным.

Если говорить подробнее о функциях, реализуемых на рабочих местах операторов, то среди них можно выделить две группы:

1) Регистрация клиента (заключение договора между банком и клиентом об открытии карточного счета). В этом случае рабочее место оператора должно обеспечивать:

- ввод персональной текстовой информации о клиенте;
 - печать текста договора между клиентом и банком об открытии счета и выпуске карты;
 - ввод графических данных: либо фотографирование клиента, либо считывание с произвольного носителя (компакт-диск, флэш-память, мобильный телефон) изображения, которое клиент хотел бы видеть на своей карте с индивидуальным дизайном;
 - ввод клиентом ПИН-кода, который будет в дальнейшем использован для выпуска карты и работы клиента с картой и счетом;
 - генерацию заказа на выпуск карты;
 - печать в конце рабочего дня отчета о выполненных операциях и действиях оператора данного рабочего места.
- 2) Выпуск карты и передача ее клиенту:**
- персонализация карты;
 - процедура передачи клиенту карты и заполнения клиентом формы о ее получении и отсутствия претензий к внешнему виду;

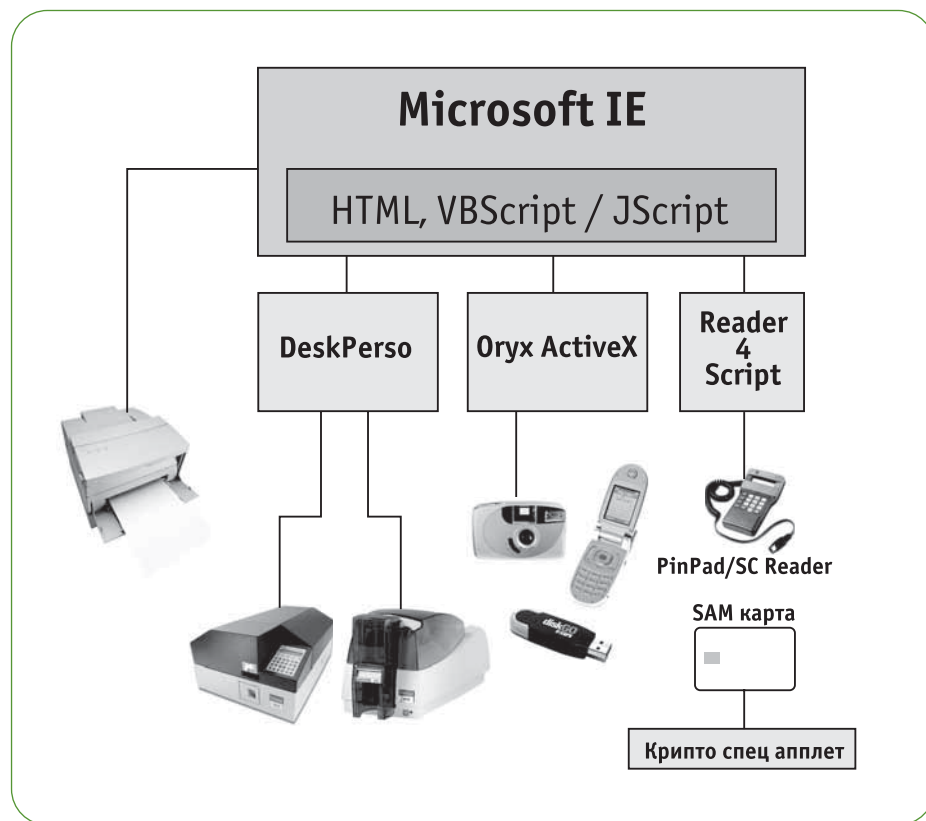


Рис. 2. Структура программного обеспечения удаленного рабочего места

- инициация процедуры активации карточки в карточной системе банка;
- печать отчета о действиях оператора, которые были выполнены в соответствующий производственный период (рабочую смену, рабочий день).

Как уже было отмечено, обе группы функций могут быть объединены и физически выполняться на оборудовании, расположенном в удаленном рабочем месте оператора системы.

III. Программное обеспечение системы

Программное обеспечение, которое используется для реализации перечисленных выше функций, характеризуется такими параметрами, как модульность и преемственность компонент, что обеспечивает надежность таких немаловажных составляющих работы системы, как, например, управление устройствами персонализации (см. рис. 2). Все программные компоненты, входящие в состав сис-

темы, подразделяются на работающие в составе удаленного рабочего места оператора и на компоненты, используемые в центральном офисе банка. К их числу относятся такие широко апробированные программные продукты, как DeskPerso (контроллер настольных устройств персонализации), SmartDataCenter (программное обеспечение подготовки EMV-данных), сервер SCPE и скрипты персонализации чиповых карт, а также другие традиционно используемые эмитентами программы и их отдельные компоненты.

В состав программного обеспечения удаленного рабочего места оператора входят:

- 1) для управления устройствами персонализации – программное обеспечение DeskPerso, хорошо зарекомендовавшее себя эффективной работой более чем у тысячи заказчиков;
- 2) для сбора информации о клиенте – компоненты системы Oryx, обеспечивающие работу с различными устройствами

для ввода и хранения текстовых и графических изображений;

- 3) для взаимодействия с SAM-картой и устройством ввода секретных кодов – модуль Reader4Script – компонента, которая включается в состав программного обеспечения SCPE – сервера управления персонализацией карт с микросхемой, широко используемого во всех проектах выпуска EMV-карт.

Программный код, работающий в рамках MS Internet Explorer (HTML, VBScript / Jscript), реализует прикладные функции удаленного рабочего места оператора и осуществляет взаимодействие со стандартными модулями, обеспечивающими управление персонализационным оборудованием, ввод изображений с широкой номенклатурой устройств и носителей, взаимодействие с устройством ввода ПИН-кода и идентификации оператора удаленного рабочего места.

Компоненты программного обеспечения, представленные на рис. 2, удовлетворяют требованиям модульности и преемственности, являются стандартными, входят в состав популярных программных систем управления персонализацией, поставляемых группой компаний КАРТ-ХОЛЛ, в том числе в рамках проектов выпуска EMV-карт, и зарекомендовали себя как современное надежное программное обеспечение. Принцип модульности создания программного обеспечения удаленного рабочего места, во-первых, упрощает процедуры, связанные с инсталляцией; во-вторых, повышает надежность; в-третьих, обеспечивает использование всех тех функций, которые обычно предоставляются пользователям отдельных программных решений в рамках единой системы удаленного выпуска EMV-карт.

IV. ПИН-пад и SAM-карта

Одним из ключевых элементов, используемых в оборудовании удаленного рабочего места, является ПИН-пад со специализированной SAM-картой. Микропроцессорная SAM-карта позволяет решить ряд

важнейших задач в системе удаленного выпуска EMV-карт. Рассмотрим эти задачи более подробно.

Работа оператора удаленного рабочего места начинается с процедуры аутентификации. Только после того как оператор введет на клавиатуре ПИН-пада свой пароль и последний будет успешно верифицирован в SAM-карте, рабочее место становится активным – т.е. способным выполнять прикладные функции.

SAM-карта хранит информацию о том, какие функциональные возможности на данном рабочем месте будут доступны оператору. С ее помощью определяется конфигурация и топология удаленных рабочих мест. Например, администратор системы имеет возможность подготовить набор SAM-карт таким образом, что на рабочем месте №1 будет разрешен только ввод информации о клиенте и печать договора, на рабочем месте №2 будут доступны функции персонализации карт и передачи их клиентам, а рабочее место №3 будет объявлено универсальным, с возможностью выполнения всех вышеперечисленных функций.

Помимо этого, SAM-карта обеспечивает хранение ключей и шифрование с их помощью информации, передаваемой от удаленного рабочего места в центральный офис и обратно. В микросхеме SAM-карты хранятся криптографические ключи 2 типов:

- используемые для шифрования ПИН-кода, введенного клиентом, с целью его последующей передачи в центральный офис системы для расчета проверочных величин и использования в данных для персонализации EMV-приложения,
- используемые для шифрования всех индивидуальных данных клиента и данных, необходимых для персонализации карты, которыми обмениваются удаленное рабочее место и ядро системы.

Таким образом, реализуется прикладная защита уникальными ключами всей информации, которой обмениваются удаленное рабочее место и центральный

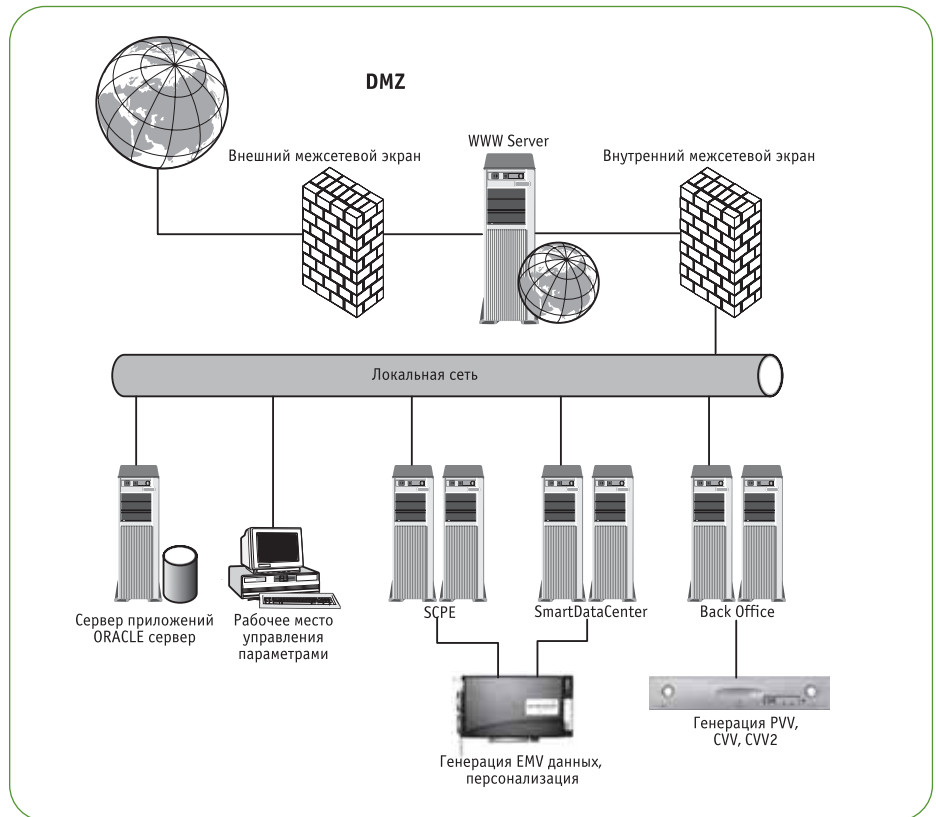


Рис. 3. Компоненты системы центрального офиса

офис. Поскольку процедуры шифрования выполняются в микропроцессоре SAM-карты, ключи, используемые для защиты данных и ПИН-кода клиента, не покидают SAM-карту, что обеспечивает выполнение современных требований безопасности при шифровании данных.

Стоит отметить, что в состав рассматриваемой системы входит рабочее место, реализующее процедуры выпуска SAM-карт, определения ПИН-кода операторов, которые будут использовать SAM-карты на удаленных рабочих местах, для учета SAM-карт, а также для загрузки безопасным образом в SAM-карты ключей защиты данных.

V. Архитектура центрального офиса

Система выпуска карт в присутствии клиента, имея собственные прикладные программные модули, расположенные в центральном офисе, взаимодействует с известными, хорошо зарекомендовавшими се-

бя решениями для подготовки данных и выпуска EMV-карт. В качестве базовой для построения системы была выбрана технология, применяющаяся при построении web-приложений. Интерфейсом между элементами центральной части системы и удаленными рабочими местами является web-сервер, который расположен в так называемой демилитаризованной зоне (рис. 3). Для его защиты от попыток несанкционированного наружного доступа предусматривается использование внешнего межсетевого экрана. В свою очередь, для повышения уровня защищенности и надежности работы компьютеров, подключенных к локальной сети центрального офиса банка, предполагается наличие внутреннего межсетевого экрана, устанавливаемого между web-сервером и прикладными серверами, а также системами центрального офиса. При этом технологические решения, использованные при создании сервера приложений, предусматривают работу через межсетевые экраны

и могут успешно функционировать в условиях ряда ограничений, которые диктуются требованиями безопасности, такими как, например, направление соединений, устанавливаемых между сервером приложений и компонентами, работающими под управлением web-сервера.

Возвращаясь к архитектуре компонент системы удаленного выпуска EMV-карт в присутствии клиента и других систем, эксплуатирующихся в центральном офисе банка, следует отметить, что в рамках системы имеется также сервер приложений, объединенный с технологической базой данных, которая:

- обеспечивает реализацию прикладных функций системы;
- содержит описание топологии удаленных рабочих мест, тех или иных функций, которые на них выполняются;
- содержит информацию о выпущенных SAM-картах и фактах их выдачи сотрудникам банка, о хранящихся в них ключах и сертификатах;
- обеспечивает ведение очередей и промежуточное хранение данных в виде записей, полученных от удаленных рабочих мест, для открытия карточных счетов;
- генерирует данные для выпуска карты;
- инициирует взаимодействие с системой бэк-офиса банка, с системой подготовки EMV-данных и системой управления персонализацией микросхемы карты клиента.

Схема, приведенная на рис. 4, иллюстрирует процессы, происходящие в системе в момент получения от удаленного рабочего места запроса на регистрацию клиента и генерацию данных. После того как такой запрос поступил, формируются соответствующие файлы, формат которых специфичен для того или иного бэк-офиса (например, для бэк-офисного решения TietoEnator будет сформирован один набор файлов, для бэк-офиса Open Way – другой набор файлов, для бэк-офиса ACI – третий). Запрос передается в бэк-офис банка для выполнения процедур, связанных с открытием счета, генерацией данных для выпуска карты и т. д. В отличие от широко использу-

емых сегодня схем характерной особенностью данной процедуры в рамках рассматриваемой системы является то, что данные запроса содержат в себе зашифрованный ПИН-блок со значением ПИН-кода, который пользователь выбрал для своей будущей карты и ввел в процессе регистрации на удаленном рабочем месте. В ответ на файловые запросы бэк-офис возвращает в систему данные, необходимые для выпуска карты: информацию для эмбоссирования, для записи на магнитную полосу, а также возможные дополнительные параметры. В ходе следующего логического шага система подготовки EMV-данных – хорошо известный комплекс SmartDataCenter – осуществляет генерацию параметров EMV-приложения для этой карты. В случае, если бэк-офис, эксплуатирующийся в банке, выполняет функции генерации EMV-параметров, то SmartDataCenter задействует минимум своих возможностей. Если же бэк-офис генерирует данные только для магнитной полосы, SmartDataCenter выполняет все необходимые действия для создания набора данных для персонализации микросхемы карты.

Полученные в ходе такого взаимодействия данные попадают в сервер базы данных системы выпуска карт и хранятся в нем до тех пор, пока с удаленного рабочего места не придет запрос на выпуск карты. В ответ на этот запрос удаленное рабочее место получает всю информацию, необходимую для выпуска карты, за исключением данных для микросхемы: данные для записи на магнитную полосу, графическую информацию (в случае выпуска карты с индивидуальным дизайном), значения полей, которые должны быть нанесены на карту в процессе эмбоссирования, и т. д.

Если описываемая система используется для выпуска EMV-карт, то в процессе персонализации карты на удаленном рабочем месте в тот момент, когда последовательность технологических операций подразумевает инициализацию микросхемы, удаленное рабочее место генерирует

новый запрос на получение информации для записи в микросхему (см. рис. 5). Этот запрос передается сервером приложений на сервер управления персонализацией микросхемы карты клиента. Там происходит генерация всех требуемых сессионных ключей. После этого данные, уже непосредственно предназначенные и зашифрованные для записи на индивидуальный экземпляр чиповой карты, передаются на удаленное рабочее место. Тем самым решается проблема, связанная с распределением по рабочим местам набора ключей, необходимых для выполнения процедур персонализации микросхемы. Эти ключи не используются на удаленных рабочих местах, а хранятся и применяются централизованно, что повышает безопасность системы в целом и ее криптографическую защищенность.

Уровень обеспечения безопасности удаленного рабочего места повышается за счет принятия следующих мер:

- 1) выполнения аутентификации оператора путем предъявления пароля к SAM-карте перед каждым началом работы на удаленном рабочем месте;
- 2) шифрования ПИН-кода клиента DES-ключами двойной длины в соответствии с требованиями стандартов, в первую очередь ISO 9564;
- 3) использования цифровой подписи и шифрования информационного обмена между удаленным рабочим местом и ядром системы. Защита данных является двунаправленной, т. е. шифруются как анкетные данные, заявление и ПИН-код клиента, так и данные для персонализации карты. При этом применяются криптографические ключи, уникальные для каждого удаленного рабочего места;
- 4) применения стандартных для информационных технологий методов и средств защиты, таких как построение виртуальных частных сетей (vpn), использование протокола HTTPS.

Комплексное принятие всех этих мер обеспечивает работу системы в соответствии с требованиями безопасности, предъ-

являемыми современными стандартами, такими как Payment Card Industry Data Security Standart, версия 1.1 (сентябрь 2006г.);

Решения, используемые при проектировании системы в целом, обеспечивают требуемый уровень безопасности за счет:

- централизованного хранения и использования разнообразных наборов ключей (так называемых master-ключей), применяемых для генерации данных для магнитной полосы, и разнообразных наборов ключей, которые требуются при генерации данных для EMV-приложений;
- использования на каждом рабочем месте SAM-карты, что обеспечивает применение уникальных ключей защиты информации при обмене по каналам связи между ядром системы и удаленными рабочими местами;
- четкого управления функциональностью удаленного рабочего места, поскольку SAM-карта содержит индивидуальный для данного рабочего места перечень прикладных операций;
- строго учета операций, выполненных на каждом рабочем месте, ведущегося в ядре системы, что позволяет в любой момент времени произвести аудит – проконтролировать, какие процедуры, на каком рабочем месте и с участием какого оператора были выполнены.

VI. Выпуск карт в присутствии клиента

Подводя итоги, проанализируем, каким образом и насколько эффективно система выпуска карт, предлагаемая ЗАО “ПРОНИТ”, позволяет достичь тех целей, которые были сформулированы нами в начале настоящей статьи.

Требование к простоте оборудования рабочих мест операторов удовлетворяется за счет использования стандартного персонализационного оборудования. Применение такого программного решения, как DeskPerso, на удаленном рабочем месте предоставляет возможность управлять любым персонализационным оборудованием, благодаря чему можно вы-

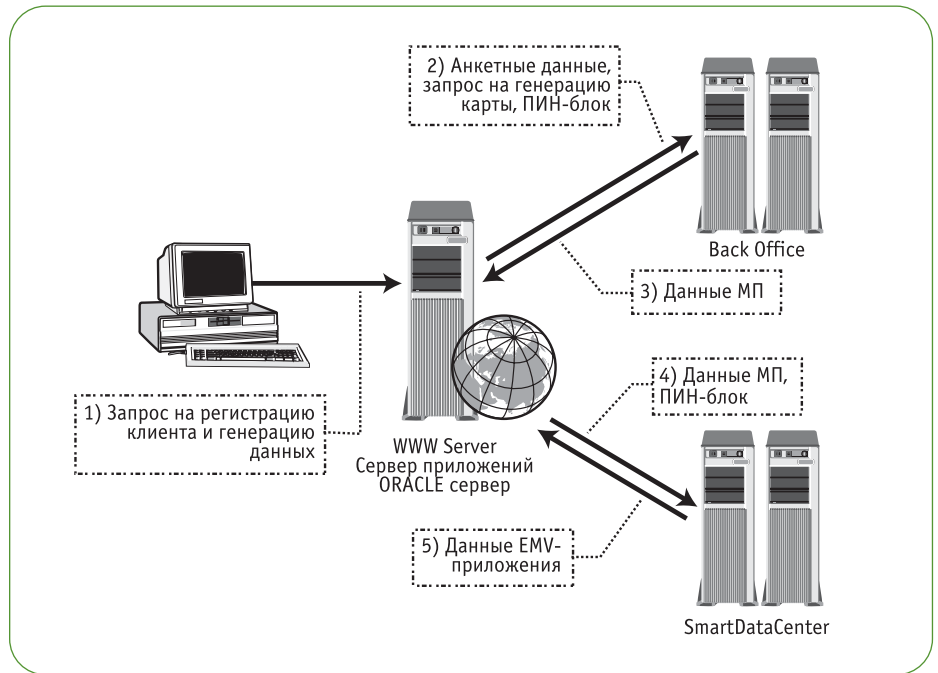


Рис. 4. Взаимодействие компонент системы при регистрации заявки

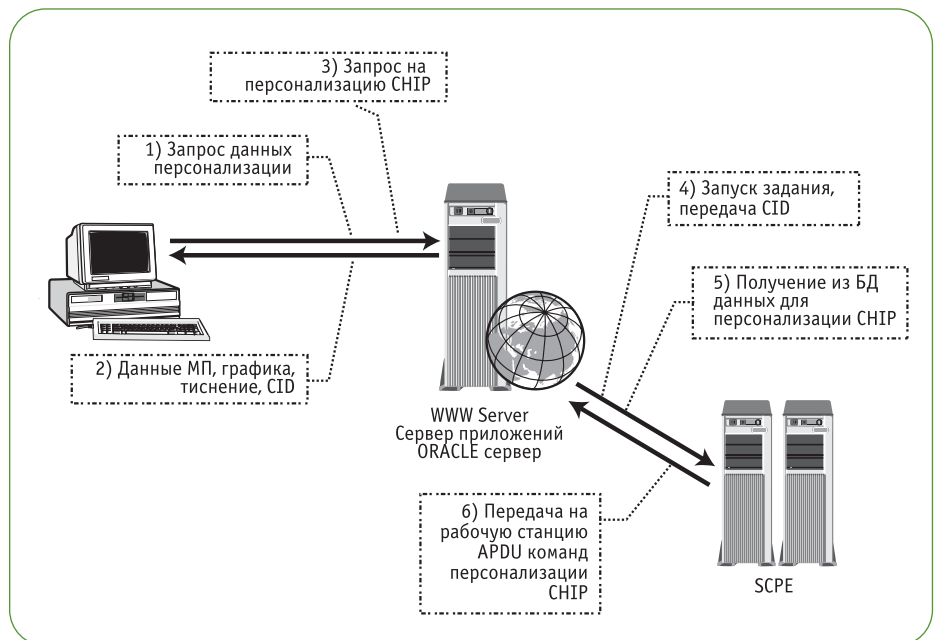


Рис. 5. Взаимодействие компонент системы при выпуске EMV-карты

брать наиболее простое и демократичное по стоимости. Возможность использования на удаленных рабочих местах широкой номенклатуры технологического оборудования для ввода и/или копирования графической информации позволяет в каждом конкретном случае выбрать тот перечень оборудования, который уже

имеется в банке, либо тот, который представляется оптимальным в соответствии с конкретными бизнес-потребностями пользователя, тем самым упростив задачу формирования рабочего места.

Предлагаемое решение не требует применения стационарных криптографических устройств непосредственно на

удаленных рабочих местах для безопасного выпуска карт, что также обуславливает простоту оборудования удаленных рабочих мест.

Требования к легкости и оперативности развертывания удаленных рабочих мест удовлетворяются за счет универсальности программного обеспечения, применяемого на удаленном рабочем месте, что обеспечивает для сотрудников IT-департамента банка ординарность операций по созданию экземпляров вычислительных средств, используемых на удаленных рабочих местах. Поскольку функционал рабочего места определяется не номенклатурой программного обеспечения, а информацией, хранящейся в SAM-карте, то “клонирование” комплектов аппаратуры для создания удаленных

ЗАО “ПРОНИТ” представляет принципиально новое персонализационное решение для “мгновенного” выпуска карт в присутствии клиента, обладающее целым рядом важных преимуществ

рабочих мест является простой и нетрудоемкой задачей.

Как известно, чем сложнее настройки, тем выше вероятность возникновения ошибок при их выполнении, соответственно, тем больше вероятность уязвимости системы. Использование стандартных протоколов, применяемых в Интернете, таких как HTTPS, обеспечивает простоту в конфигурации межсетевых экранов, исключает возникновение специальных требований к их настройкам, что упрощает как деятельность сотрудников IT-департамента, выполняющих эти настройки, так и контроль действий данных сотрудников, что также немаловажно.

Следует отметить, что, рассматривая выполнение современных требований к уровню обеспечения безопасности и защищенности данных, мы говорим о том, что каждое рабочее место начинает функционировать только после аутентификации оператора путем предъявления пароля; о том, что мы обеспечиваем тотальное шифрование данных, пе-

редаваемых между различными территориально удаленными компонентами системы, с помощью уникальных для каждого рабочего места ключей; об использовании протоколов и средств защиты (виртуальные частные сети, протокол HTTPS), которые и де-факто, и де-юре стали технологическими стандартами в области передачи данных; и, наконец, о централизованном хранении ключей и подготовке данных, которые требуют их применения, в центральном офисе в защищенной сети с использованием предназначенных для этого аппаратных решений.

Удобство настройки и мониторинга работы рассматриваемой нами системы обеспечивается за счет тех же архитектурных решений, которые уже неодно-

кратно были перечислены в рамках настоящей статьи. К ним относятся: управление функциональностью рабочего места с помощью параметров, записываемых в SAM-карту; централизованное хранение информации об операциях, выполнявшихся на удаленных рабочих местах, соответственно, возможность аудита и мониторинга в реальном масштабе времени действий, выполняемых в системе; единая система настройки параметров и подготовки SAM-карт, которая осуществляется в центральном офисе; развитая система построения отчетов, которая имплементирована в систему, что позволяет получить ответ на любой вопрос, что, когда и где в данной системе происходило.

VII. Заключение и выводы

Итак, ЗАО “ПРОНИТ” представляет принципиально новое персонализационное решение для “мгновенного” выпуска карт в присутствии клиента, обладающее целым рядом важных преимуществ:

- 1) Поддерживается персонализация как “магнитных”, так и EMV-совместимых карт.
- 2) С одной стороны, решение базируется на достаточно апробированных и широко применяемых для взаимодействия с различными хостовыми системами программных продуктах ЗАО “ПРОНИТ”, обеспечивающих полный цикл персонализации, включая “удаленную” персонализацию:
 - подготовку данных для карт с магнитной полосой и печать ПИН-конвертов;
 - подготовку EMV-данных;
 - собственно персонализацию;
 - тестирование выпущенных чиповых карт.
- 3) ...с другой стороны, решение может быть достаточно легко адаптировано к взаимодействию с другими программными комплексами центрального персобиюро, обеспечивающими подготовку данных для персонализации.
- 4) Решение обеспечивает различные схемы персонализации, в том числе:
 - полная персонализация карты в присутствии клиента (т. н. банковский метод);
 - предперсонализация в центральном персобиюро с последующей доперсонализацией на месте выдачи;
 - предперсонализация EMV-приложения с активацией на месте выдачи;
 - персонализация карт с фотографией владельца или карт индивидуального дизайнера.
- 5) Экономическая эффективность (при выполнении необходимых требований к обеспечению безопасности) достигается за счет отсутствия в точках персонализации и выдачи карт дорогостоящих HSM, ввода ПИН-кода самим клиентом с использованием ПИН-клавиатуры и SAM-карты, а также подготовки EMV-данных в центральном персобиюро в режиме реального времени.
- 6) Решение поддерживает всю линейку персонализационного настольного оборудования Datacard (эмбоссеры и графические принтеры), а также PC/SC устройства чтения/записи смарт-карт.