

© ООО «СКАНТЕК»

ПЛАТЕЖНАЯ СИСТЕМА *SMARTPAY*™

ОПИСАНИЕ СИСТЕМЫ

ВЕРСИЯ 1.00

Москва 2017 г.

Содержание

Содержание	2
Сокращения	3
Структура системы	4
Возможности процессингового центра.....	4
Адресование объектов в системе	5
Курсы валют.....	6
Ограничения на состав покупаемых товаров.....	6
Лимиты.....	6
Блокировка обслуживания карт.....	6
Платежные операции.....	7
Управление обслуживанием карты на терминалах со стороны эмитента	8
Рекламные сообщения.....	9
Обработка запросов терминалов эквайером	9
Контроль сверки итогов	10
Взаимодействие с эмитентами.....	10
Журналы и архивы.....	11
Персонализация платежных карт	11
Карты персонализации и типы платежных карт	12
Организация защиты информации в системе	13
Проверка ПИН.....	13
Начальная установка ПИН на карте.....	13
Ключи и организация их хранения. LSM сервера обработки.....	14
Пул LSM	16
Обмен с терминалами.....	16
Разграничение доступа к информации и контроль работы операторов	17
Структура программных и технических средств процессингового центра	18
Сервер обработки ПЦ	18
Рабочее место оператора ПЦ	19
Рабочее место администратора LSM	20
Рабочее место персонализации платежных карт	20
Требования к среде функционирования ПЦ	20

Сокращения

PM - рабочее место
АЗС - автозаправочная станция
АТС - Application Transaction Counter (счетчик транзакций карты)
БД - база данных
ПИН - Personal Identification Number (пароль клиента для аутентификации карты клиента в системе)
ПО - программное обеспечение
ПЦ - процессинговый центр системы
СУБД – система управления базами данных
AID - идентификатор приложения EMV
BNC - счетчик сверки итогов
СА - центр авторизации сертификатов SSL
СО - сервер обработки процессингового центра
ЛМК - ключ шифрования ключей, хранящихся в базе данных
LSM - модуль обработки секретной информации
КЕК - ключ шифрования ключей, загружаемых извне
KSN - серийный номер ключа шифрования PIN блока
PAN - Primary Account Number (идентификационный номер платежной карты)
РЕК - ключ для шифрования PIN блоков, передаваемых терминалом по каналам связи при on-line проверке ПИН
PIN блок - формат хранения и передачи ПИН клиента (преобразованного с помощью PAN)
РРК - ключ для шифрования PIN блоков, хранящихся в базе данных
RID - идентификатор зарегистрированного провайдера приложения EMV
RRN - регистрационный номер запроса
SmartPay - платежная система
SSL - криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером
УКРТ - Unique Key Per Transaction (механизм шифрования PIN блоков с генерацией уникального сессионного ключа на транзакцию)

Структура системы

Система SmartPay обеспечивает проведение безналичных платежей на АЗС за купленное топливо или сопутствующие товары.

Данное решение ориентировано на топливные проекты, каждый из которых поддерживает работу небольшого числа АЗС.

Использование «бюджетного» процессингового решения позволяет быстро развернуть систему и упрощает ее эксплуатацию. В случаях миграции с решений других вендоров возможно сохранение бизнес-подходов.

Основные компоненты:

- Процессинговые центры системы (ПЦ);
- программное обеспечение для различных моделей терминалов Ingenico;
- дуальные смарт-карты, соответствующие стандарту EMV.

В системе может быть один или несколько процессинговых центров.

Обеспечивается возможность объединения в единую систему ранее независимо функционирующих однопроцессинговых систем с возможностью обслуживания платежных карт всех ПЦ на всех терминалах объединенной системы.

Платежные операции выполняются на платежных терминалах, устанавливаемых на АЗС.

На одной АЗС может быть установлено несколько терминалов.

Обмен между терминалами и ПЦ и между ПЦ осуществляется по TCP каналам.

Платежные операции выполняются с использованием платежных карт.

Платежные карты могут работать как по контактному, так и по бесконтактному интерфейсу. Выбор применяемого при конкретной платежной операции интерфейса осуществляется с учетом типа терминала, на котором выполняется операция, оператором АЗС/клиентом.

Возможности процессингового центра

Процессинговые центры могут выполнять функции эмитента и эквайера.

Эквайер системы SmartPay обеспечивает выполнение следующих функций:

- учет в базе данных терминалов и АЗС, обслуживаемых данным эквайером;
- прием транзакций, поступающих от терминалов, обслуживаемых данным эквайером, и доведение их до процессингового центра эмитента;
- получение ответов от процессинговых центров эмитента и доведение их до терминалов, выдавших запрос;
- формирование отчетов о выполненных платежных операциях по картам внешних эмитентов;
- блокировку обмена информацией с внешними процессинговыми центрами;
- защиту от подделки транзакций;
- защиту от повторов и обгонов транзакций при обмене между терминалами и процессинговым центром.

Процессинговый центр эмитента обеспечивает:

- ведение счетов клиентов системы;
- контроль лимитов покупки топлива или других товаров, установленных клиенту;

- контроль покупки с помощью платежных карт только разрешенных в системе типов товаров;
- сбор и учет платежных транзакций, поступающих от терминалов и ПЦ эквайеров, на счетах клиентов и в лимитах покупки топлива клиентов;
- предоставление отчетов о выполненных транзакциях эмитентам, АЗС и ПЦ эквайеров;
- защиту от подделки транзакций;
- защиту от повторов и обгонов транзакций при обмене между терминалами и процессинговым центром.

Для каждого клиента в базе данных процессингового центра эмитента создается счет клиента, на который эмитентом заносятся средства, в рамках которых клиент может осуществлять покупки товаров с помощью платежной карты.

Под эмитентом понимается любая организация, в интересах которой в ПЦ персонализируются платежные карты клиентов и обеспечивается проведение безналичных платежей с использованием указанных карт.

Эмитент может разделить клиентов (счета) на категории. Клиент может иметь только одну категорию. Условия обработки транзакций в ПЦ по счетам различной категории могут быть разными.

К одному счету клиента может быть привязано несколько платежных карт. Однако действующей картой может быть только одна. После выпуска новой карты клиента при первом ее использовании все остальные карты клиента блокируются в ПЦ.

Как правило, процессинговый центр выполняет функции и эквайера и эмитента.

Процессинговый центр обслуживает непосредственно подключенные к нему терминалы, учитывает платежные транзакции, поступающие от «своих» терминалов и внешних ПЦ на счетах «своих» клиентов. Если платежная операция выполнена по карте другого процессингового центра транзакция перенаправляется в этот процессинговый центр.

С помощью настроек ПЦ можно обеспечить, чтобы ПЦ выполнял функции только эмитента/эквайера. или обслуживал только свои карты с терминалов, подключенных непосредственно к данному ПЦ.

Адресование объектов в системе

Идентификатор процессингового центра кодируется строго 6 цифрами, причем первая цифра кода не должна равняться 0.

Терминалы адресуются локально в рамках каждого процессингового центра, к которому они подключены. Идентификатор терминала кодируется 5 цифрами (0-65535).

Эмитенты адресуются локально в рамках каждого обслуживающего их процессингового центра эмитента. Идентификатор эмитента кодируется 4 цифрами (0-9999).

Адресование карт клиентов и эмитентов осуществляется в соответствии со стандартами EMV. Карта клиента идентифицируется с помощью PAN (ISO 7812-1).

PAN содержит 19 цифр и имеет следующую структуру: ППППППДДЭЭЭЭNNNNNNNC. Здесь ПППППП - идентификатор процессингового центра, ДД-тип программного продукта, ЭЭЭЭ - код эмитента, NNNNNN - номер карты эмитента, C -контрольный разряд.

Транзакции, передаваемые эквайером эмитенту, передаются от имени ПЦ эквайера. Т.е. в качестве адреса отправителя указывается идентификатор ПЦ эквайера.

При учете в базе данных эквайера транзакций внешних эмитентов в качестве идентификатора эмитента фиксируется идентификатор процессингового центра эмитента для данной транзакции.

При учете в базе данных эмитента в качестве идентификатора эмитента фиксируется локальный код эмитента.

Курсы валют

В системе платежные операции на разных терминалах могут выполняться в разных валютах. В ПЦ эмитента хранится справочник курсов валют для пересчета стоимости покупки из валюты платежа к валюте счета. Поддерживаться работа с несколькими версиями справочника курсов валют. К каждому терминалу может применяться только одна версия справочника.

Ограничения на состав покупаемых товаров

Обеспечивается возможность ограничения состава товаров или групп товаров, которые могут купить с использованием платежной карты клиенты различных категорий.

В ПЦ эмитента для локального кода эмитента и категории клиента (всех категорий) хранится список разрешенных товаров/групп товаров. Терминал вместе с платежной транзакцией передает код покупаемого товара.

Если данного товара в списке разрешенных товаров данной категории клиента нет и если этот список не пуст, то в выполнении платежной транзакции в ПЦ будет отказано.

Если список разрешенных товаров пуст, то разрешены для приобретения все товары.

Код товара в системе содержит до 9 цифр.

Для каждого товара определяется группа, в которую он входит. Ограничения могут устанавливаться, как на отдельные товары, так и на группы товаров.

Лимиты

В ПЦ эмитента обеспечивается возможность установки эмитентом или оператором ПЦ лимитов на конкретный срок в днях или месяцах на покупку конкретного топлива/товара.

Администратором ПЦ могут быть установлены лимиты на покупку товаров в целом на эмитента. При контроле данного лимита учитываются операции всех клиентов данного эмитента.

Лимиты могут устанавливаться на количество купленного товара или его стоимость. Стоимостной лимит устанавливается в определенной выбранной валюте. Стоимостной лимит применяется к данному счету, если валюта счета совпадает с валютой лимита.

Стоимостной лимит может быть установлен также на все купленные товары.

Лимиты могут быть лонгируемые и не лонгируемые. Для лонгируемого лимита по завершению текущего периода действия лимита, устанавливается тот же лимит на следующий период. Срок действия лимита может устанавливаться в днях или в месяцах. Лимиты могут устанавливаться на всех клиентов эмитента и клиентов заданной категории.

Если клиент превысил один из установленных для него лимитов, в выполнении платежной операции ему будет отказано.

Блокировка обслуживания карт

У эквайера может быть заблокирована оператором ПЦ передача транзакции конкретному ПЦ эмитента.

В ПЦ эмитента обслуживание карт может быть заблокировано либо оператором процессингового центра, либо эмитентом. Если блокировка счета установлена оператором, то информация об этом передается эмитенту. Блокировка может быть установлена на уровне:

- эмитента (блокируются все карты эмитента);
- счета клиента (блокируются все карты данного клиента);
- карты (блокируется одна карта).

На карте и в базе данных ПЦ хранится срок действия карты (дата начала действия и дата конца действия). Срок действия карты, записанный на карте, проверяется терминалом. Срок действия карты, записанный в БД, проверяется в ПЦ при обработке транзакций. Срок действия карты, записанный на карте, может отличаться от срока действия карты, записанного в базе. Срок действия карты в БД может быть изменен оператором системы.

Платежные операции

Состав и кодирование сообщений обмена между терминалом и ПЦ соответствует ISO-8583.

Терминал может передать в процессинговый центр следующие типы запросов:

- запрос баланса карты;
- запрос авторизации покупки;
- запрос отмены авторизации покупки;
- запрос подтверждения покупки;
- транзакция частичного или полного возврата покупки;
- транзакция сверка итогов.

В ответ на запрос баланса ПЦ выдает количество средств на счете в валюте терминала. Кроме того, в ответе выдается до 15 наколенных для данного клиента сумм по установленным для него лимитам.

В запросе авторизации терминалом передается код товара, количество, цена и стоимость товара в валюте платежа. Если до начала платежа не известно количество и стоимость покупаемого товара (например, при заправке до полного бака), то передается предельные количество и стоимость товара, определяемые оператором терминала.

ПЦ эмитента выдает разрешение или запрет на выполнение платежной операции исходя из наличия средств на счете, установленных лимитов и ограничений на покупаемые товары для данного клиента.

При отказе он сообщает терминалу свою предельную (авторизованную) стоимость покупки в валюте платежа, которую клиент может потратить.

Если ПЦ выдает разрешение на выполнение платежной операции, стоимость покупки учитывается на счете клиента и во всех лимитах клиента в системе.

Если терминал не получил ответ на запрос авторизации, то он выдает запрос отмены авторизации. Запрос отмены может быть выдан терминалом также после получения положительного ответа от ПЦ в случае, если не удалось завершить операцию покупки. Такой запрос отмены может быть выдан до выдачи подтверждения покупки и выполнения сверки итогов.

При получении запроса отмены авторизации ПЦ откатывает зарезервированные средства на счете клиента и в лимитах.

После выполнения покупки терминалом в ПЦ должна передаваться (финансовая) транзакция подтверждения покупки, содержащая действительное количество и сумму платежа.

По этой транзакции лишние (зарезервированные) средства возвращаются на счет клиента и списываются из лимитов клиента.

Терминал может передавать транзакции подтверждения покупки или возврата в ПЦ как в on-line режиме, так и в off-line режиме.

Транзакции off-line режима накапливаются в off-line буфере терминала и разгружаются в ПЦ по on-line каналу при первой возможности. Транзакции разгружаются в порядке поступления их в off-line буфер.

Транзакция подтверждения покупки выдается в off-line режиме в следующих случаях:

- если терминал не может выдать транзакцию авторизации покупки в on-line и карта и терминал подтвердили возможность выполнения транзакции в off-line режиме;
- если не получен ответ от ПЦ на транзакцию авторизации, и карта и терминал подтвердили возможность выполнения транзакции в off-line режиме.

Данная возможность реализуется только для операций, выполняемых по контактному интерфейсу.

Запрос возврата может быть передан терминалом в ПЦ только после успешной выдачи (on-line или off-line) подтверждения покупки, по которой осуществляется возврат.

Отмена запроса подтверждения покупки может осуществляться только транзакцией возврата покупки.

Если запрос подтверждения покупки находится в off-line буфере, запрос возврата также передается в off-line режиме.

При получении запроса возврата в ПЦ эмитента проверяется наличие подтверждения покупки, по которой осуществляется возврат, а также, что сумма возврата (сумма всех возвратов) не превышает начальную стоимость товара. Сумма возврата возвращается на счет и списывается из накопительных периодов лимитов, установленных для данного клиента.

Запрос сверки итогов формируется при закрытии смены терминала. На терминале должен вестись счетчик сверки итогов (BNC).

При выдаче нового запроса сверки итогов BNC увеличивается на 1. Запрос сверки итогов содержит подтверждаемое BNC. Запрос сверки итогов может быть выдан терминалом в ПЦ, только если у него нет не завершенного обмена по карте клиента и нет в off-line буфере транзакций с BNC меньшим или равным подтверждаемому.

С помощью запроса сверки итогов обеспечивается синхронизация состава обработанных транзакций в терминале и ПЦ. После получения запроса сверки итогов ПЦ считает, что от терминала больше не может поступить каких-либо запросов отмены или подтверждения покупки по платежным операциям с подтвержденным BNC.

Транзакции возврата могут передаваться и обрабатываться в ПЦ после сверки итогов, в которой учтена начальная операция.

Управление обслуживанием карты на терминалах со стороны эмитента

В БД эмитента для каждого клиента может храниться *Порог остатка на счете on-line операций*. Если остаток средств на счете меньше указанного порога, то в ответ на запрос авторизации включается признак *Set Go Online on next transaction* (следующая

транзакция должна передаваться только в on-line режиме). Данный признак записывается на карту и таким образом препятствует выполнению платежной операции в off-line, где бы она ни выполнялась. Указанный признак устанавливается на карте также в том случае, если карта, счет или эмитент заблокированы.

Если код блокировки в БД имеет значение *Изъят из обращения*, на карте устанавливается признак Card Block. После чего доступ к карте будет заблокирован на любом терминале системы.

Признаки записываются на карту только при работе по контактному интерфейсу.

Рекламные сообщения

Ответ на успешно обработанный запрос авторизации или запрос баланса может сопровождаться одним или несколькими рекламными сообщениями. Рекламные сообщения распечатываются в чеке. Максимальная длина всех рекламных сообщений, передаваемых в ответе терминалу - 512 байт. Для разных эмитентов может быть установлен разный состав рекламных сообщений. Для каждого рекламного сообщения может быть установлен срок его жизни. Рекламное сообщение передается на терминал, если его срок жизни еще не истек.

Обработка запросов терминалов эквайером

При поступлении запроса от терминала ПЦ осуществляет контроль правильности синтаксиса транзакций и соответствие порядка их поступления от терминала протоколу обмена.

При получении запроса баланса от терминала ПЦ эквайера открывает новое соединение с ПЦ эмитента и передает ему полученный запрос. После получения ответа, ответ доводится до терминала.

При получении запроса авторизации покупки ПЦ эквайера фиксирует его в своей БД, открывает нового соединения с ПЦ эмитента и передает ему запроса авторизации. После получения ответа, ответ фиксируется в БД и доводится до терминала.

Запросы

- отмены авторизации;
- подтверждения покупки;
- возврата покупки;

поступивший от терминала фиксируются в БД, на терминал выдается положительный ответ о принятии запроса на обработку и запрос записывается в пул запросов, подлежащих передаче эмитенту. ПЦ эквайера далее сам обеспечивает гарантированную доставку запроса эмитенту.

В ПЦ эквайера может быть установлено ограничение на количество ТСП соединений, используемых при обмене с внешними эмитентами.

ПЦ эквайера при наличии свободных соединений и отсутствии в пуле запросов, ожидающих передачи, сразу устанавливает связь с ПЦ эмитента и передает ему полученное сообщение из пула.

Если свободного соединения нет, то запрос будет ждать своей очереди на передачу. Передача осуществляется по мере освобождения соединений. Запросы выбираются для передачи в порядке поступления их в ПЦ эквайера.

При получении ответа от ПЦ эмитента сообщение фиксируется в БД и удаляется из пула обмена.

Запрос сверки итогов, передаваемый в ПЦ эмитента, формируется эквайером самостоятельно исходя из значений параметров периодичности сверки итогов и времени

последней передачи запроса сверки итогов эмитенту. Запрос сверки итогов может быть передан также по команде оператора ПЦ эквайера.

Запрос сверки итогов передается от имени ПЦ эквайера. В запросе указывается текущее значение BNC эквайера для данного ПЦ эмитента.

Запрос сверки итогов эквайера содержит поле *Time reconciliation*. Данное поле определяет дату сверки итогов для данного запроса. Данное время может не совпадать с временем формирования запроса сверки итогов.

При формировании запроса сверки итогов параметру *Time reconciliation* присваивается минимальное значение даты сверки итогов терминалов эквайера (T_{min}).

При обработке запроса сверки итогов в ПЦ эмитента, если разница между текущим временем ($T_{тек}$) и *Time reconciliation* больше *Максимального временного интервала сверки итогов* (I_{max}), заданного в настройках ПЦ, то значение *Time reconciliation* приравнивается значению $T_{тек} - I_{max}$.

При обработке запроса сверки итогов в ПЦ эмитента транзакции, имеющие время *Transmission Date/Time* меньшее или равное значению поля *Time reconciliation*, считаются прошедшими сверку итогов.

Контроль сверки итогов

В ПЦ эквайера или эмитента обеспечивается возможность получения итоговых отчетов о выполненных транзакциях на терминалах или внешних ПЦ для каждого BNC сверки итогов. Отчеты хранятся в системе две недели, а затем автоматически удаляются. В отчет входят следующие данные;

- Для каждого типа операции (подтверждение или возврат), валюты платежа и каждого типа купленного товара: количество выполненных операций, суммарная стоимость всех покупок/возвратов, суммарное количество товара;
- Для каждого типа операции (подтверждение или возврат) и валюты платежа: количество выполненных операций, суммарная стоимость всех покупок/возвратов;
- Для каждой использованной валюты платежа: количество выполненных операций, суммарная стоимость всех покупок за вычетом возвратов.

Взаимодействие с эмитентами

Процессинговый центр эмитента для каждого локального эмитента формирует список обработанных транзакций, прошедших сверку итогов. В список включаются только успешно обработанные транзакции подтверждения покупки и возврата.

ПЦ передает эмитенту также отчеты о заблокированных по инициативе операторов ПЦ счетах клиентов, а также о всех изменениях, внесенных на счета клиентов операторами процессингового центра.

Процессинговый центр эквайера формирует для каждого внешнего ПЦ-эмитента отчет со списком успешно обработанных этим ПЦ транзакций подтверждения покупки или возврата.

Локальный эмитент может передавать в ПЦ эмитента следующую информацию:

- список новых клиентов, подключаемых к системе или список изменений атрибутов уже существующих клиентов;
- начисления на счет клиентов дополнительных средств;

- список заблокированных/разблокированных клиентов по инициативе эмитента;
- список изменений категории клиентов;
- список лимитов, устанавливаемых в системе для данного эмитента в целом или его категорий клиентов.

Взаимодействие ПЦ с локальными эмитентами может осуществляться с помощью:

- xml-файлов, выгружаемых ПЦ в выходной каталог системы или загружаемых из входного каталога системы;
- процедур базы данных, выполняемых внешним программным обеспечением.

Для каждого эмитента или внешнего процессингового центра отчет записывается в отдельный файл.

Загрузка файлов из входного каталога системы осуществляется автоматически. Выгрузка файлов в выходной каталог системы осуществляется в соответствии с установленным оператором системы расписанием.

На рабочем месте оператора ПЦ эмитента и эквайера обеспечивается возможность формирования и отображения отчетов о функционировании системы, в том числе:

- по операциям с конкретной картой или счетом клиента;
- о выполненных транзакциях на конкретном терминале;
- о транзакциях подтверждения покупки или возврата, при обработке которых в ПЦ эквайера или ПЦ эмитента произошла ошибка.

Обеспечивается возможность распечатать такой отчет или записать его в Excel, Word или PDF файл для дальнейшей обработки.

Журналы и архивы

Контроль обработки транзакций, поступающих от терминалов, а также контроль изменений средств на счетах клиентов осуществляется с помощью журнала операций и архива транзакций.

В журнале эмитента фиксируются все транзакции (кроме повторных), поступающие от терминалов и внешних ПЦ. В журнале эмитента фиксируются также все изменения параметров счета клиента, выполненные эмитентом или оператором системы.

В журнале фиксируется код обработки транзакций в ПЦ.

В журнале эквайера по транзакции поступившей от терминала регистрируются две записи:

- результат обработки транзакции, поступившей от терминала;
- результат передачи и обработки данной транзакции у эмитента.

Журнал не корректируется.

В архив записываются все успешно обработанные транзакции подтверждения покупки и возврата.

В ПЦ обеспечивается возможность регистрация в суточные файлы трассировки ошибочных или всех сообщений обмена с терминалами или внешними ПЦ.

Персонализация платежных карт

Процессинговый центр эмитента обеспечивает выпуск новых платежных карт клиентов по запросу операторов РМ системы взамен уже существующих карт или для новых клиентов, введенных операторами системы. Обеспечивается также персонализация карт новых клиентов, атрибуты которых поступили от эмитента в виде xml файла во входной каталог ПЦ.

Персонализация новых карт осуществляется на *Рабочем месте персонализации* ПЦ. Реализовано два варианта организации персонализации карт;

- централизованная персонализация карт;
- децентрализованная персонализация карт.

В одном процессинговом центре могут быть задействованы оба типа организации персонализации карт.

В централизованном варианте формирование файлов заявок на персонализацию карт осуществляет сервер обработки ПЦ. Взаимодействие сервера обработки и РМ персонализации осуществляется через каталоги операционной системы.

Для сервера обработки определяется каталог заявок персонализации системы с тремя подкаталогами:

- подкаталог запросов персонализации системы;
- подкаталог положительных ответов персонализации;
- подкаталог отрицательных ответов персонализации.

Аналогичные каталоги определяются для рабочего места персонализации.

При выдаче оператором РМ запроса на выпуск новой карты для заданного клиента или при обработке запроса создания нового клиента в БД фиксируется заявка на выпуск новой карты. Сервер обработки периодически просматривает таблицу заявок и при наличии новых заявок формирует файлы заявок, в подкаталоге запросов персонализации системы. Далее, сервер обработки периодически просматривает подкаталоги положительных и отрицательных ответов персонализации. При получении ответа сервер обработки фиксирует ответ в таблице заявок. Если ответ положительный в БД фиксируется вновь созданная карта.

На рабочем месте персонализации при появлении файла заявки в подкаталоге запросов персонализации информация заявки из файла отображается на экране РМ. Оператор должен установить новую карту в считыватель карт и запустить процесс персонализации. В зависимости от результата персонализации ответ записывается в подкаталог либо положительных, либо отрицательных ответов РМ.

При децентрализованном варианте персонализация карт осуществляется на рабочем месте оператора, формирующем заявки. К компьютеру рабочего места в этом случае должен быть подключен LSM, который будет выполнять криптографические операции по формированию файла заявки персонализации и при персонализации карты. Рабочее место персонализации карт должно быть развернуто на том же компьютере. При децентрализованном варианте рабочее место оператора само формирует файл заявки персонализации и выкладывает его в выходной каталог рабочего места.

На рабочем месте персонализации оператор сразу может выпустить новую платежную карту и выдать ее клиенту. Персонализация новой карты занимает порядка 15 секунд.

Вариант, в котором работает данное рабочее место оператора ПЦ (централизованном или децентрализованном) определяется настройкой рабочего места.

Карты персонализации и типы платежных карт

При персонализации на платежную карту записываются данные динамической аутентификации карты, ключи приложения EMV, необходимые для подписи транзакций картой и защиты скриптов, передаваемых из ПЦ на карту при смене ПИН. Кроме того, на карту пишется достаточно большое количество параметров, управляющих обработкой карты на различных типах терминалов и параметров управления рисками. Персонализация платежных карт осуществляется с использованием карты персонализации. На карту персонализации записываются открытый RSA ключ эмитента (Issuer Key) и его EMV сертификат, полученный на ключе CA. Кроме того,

записывается открытый и секретный ключ карты (Card Key). На карту персонализации записывается также ключ лота, на котором закрыты “чистые” карты, используемые для персонализации платежных карт. Кроме того, могут быть записаны значения наиболее общих параметров настройки. В ПЦ может быть создано несколько карт персонализации с разным набором версий ключей, разным составом и значениями параметров. Карта персонализации обеспечивает:

- объединение множества параметров настройки, находящихся на карте персонализации и поступивших в заявке персонализации;
- безопасную запись данных на персонализируемую карту.

Карта персонализации выпускается на рабочем месте оператора и передается для использования на рабочее место персонализации карт.

В ПЦ определяется один или несколько типов платежных карт. Для каждого типа определяются значения параметров, дополняющих список параметров карты персонализации до полного (кроме PAN, срока жизни карты и имени клиента на карте). Списки параметров карты персонализации и типа платежной карты могут пересекаться. В этом случае при персонализации платежной карты используется значение параметра в типе карт.

В заявке персонализации платежной карты, записываемой в БД, указываются PAN, срок жизни карты, имя клиента на карте и тип персонализируемой карты. При формировании файла заявки сервером обработки в заявку добавляются значения параметров типа карты. Кроме того, в заявку добавляются в диверсифицированные на PAN ключи приложения EMV, а также EMV сертификат ключа данной карты, полученный на ключе Issuer.

Администратор системы может определить для эмитента и его категорий клиентов тип персонализируемой карты. За счет такой предварительной настройки заявка на персонализацию для существующего клиента может формироваться оператором нажатием одной кнопки. За счет этого обеспечивается также автоматическое формирование заявок при обработке xml файла эмитента со списком новых клиентов.

Организация защиты информации в системе

Платежная карта аутентифицируется терминалом по алгоритмам CDA EMV.

Карта аутентифицируется в ПЦ эмитента с помощью передаваемых терминалом криптограмм EMV, формируемых картой на ключах, известных только карте и ПЦ эмитента.

ПЦ эмитента аутентифицируется картой при выполнении запроса авторизации по контактному интерфейсу с помощью криптограмм EMV, формируемых в ПЦ и передаваемых в ответных сообщениях на терминал.

Проверка ПИН

Правила верификации клиента на терминале задаются при персонализации платежной карты, а также определяются возможностями и настройкой терминала.

Проверка ПИН при работе по контактному интерфейсу может выполняться самой картой в off-line режиме. Для бесконтактного интерфейса ПИН передается запросом терминала и проверяется в ПЦ. В ПЦ контролируется количество не правильного предъявления ПИН.

Начальная установка ПИН на карте

Новые карты после их выпуск не содержат ПИН. На карте в этом случае установлен признак PIN not set. При отсутствии ПИН терминал передает в ПЦ запрос смены ПИН.

Для ПЦ запрос смены ПИН является обычным запросом авторизации, сформированным по контактному интерфейсу, в котором признак PIN not set установлен в 1 и в котором передан on-line PIN.

По данному запросу PIN блок, полученный в запросе, записывается в зашифрованном виде в базу данных и в дальнейшем используется для проверки on-line ПИН. Кроме того, формируется скрипт команды карты Change PIN, содержащий ПИН из полученного в запросе PIN блока.

При получении ответа от ПЦ терминал с помощью указанного скрипта устанавливает off-line ПИН на карте и сбрасывает признак PIN not set.

Ключи и организация их хранения. LSM сервера обработки

В ПЦ для выполнения криптографических операций и хранения ключей используется LSM (secure module) и карта персонализации.

LSM подключается к серверу обработки и реализуется в виде Java карты с загруженным соответствующим апплетом ПО. Физически он представляет собой USB флешку с вставленной внутрь ее Java картой (чипом Java карты).

Карта персонализации используется для персонализации платежных карт на рабочем месте персонализации. Принципы работы LSM и карты персонализации в целом одинаковые. Апплет карты персонализации обеспечивает выполнение ряда дополнительных функций, связанных с персонализацией карт.

LSM осуществляет безопасное выполнение криптографических операций: ключи и критическая с точки зрения доступа информация нигде кроме LSM в открытом виде не появляется.

В LSM хранятся следующие симметричные 3DES ключи:

- Ключ базы данных (ЛМК), предназначенный для шифрования ключей, хранящихся в базе данных;
- Ключи шифрования ключей (КЕК), предназначенные для шифрования ключей загружаемых (выгружаемых) в подсистему (например, лотовых ключей).

В базе данных ПЦ эмитента хранятся следующие 3DES ключи:

- мастер-ключ проверки криптограмм (Кас);
- мастер-ключ шифрования данных (Кс);
- мастер-ключ обеспечения целостности данных (Ки);
- базовые ключи шифрования PIN блоков, поступающих в данный процессинговый центр (РЕК);
- ключ шифрования PIN блоков клиентов в базе данных (РРК);
- ключ шифрования PIN блоков клиентов в базе данных (РРК);
- ключ лота карт.

В базе данных ПЦ эквайера хранятся следующие 3DES ключи:

- базовый ключи шифрования PIN блоков, для расшифрования PIN блоков, поступающих от терминалов данного ПЦ (РЕК);
- для каждого внешнего ПЦ диверсифицированный ключ РЕК внешнего ПЦ.

Ключ Кас используется при проверке криптограмм платежной карты (ARQC, TC, AAC), поступающих в запросах терминалов и формирования криптограмм ответов ПЦ (ARPC) на эти запросы.

Ключи Кс и Кі используются при формировании скрипта смены ПИН на карте при начальной записи ПИН на карту.

Наборы ключей Кас, Кс, Кі генерируются в целом для ПЦ, т.е. одни и те же ключи могут быть использованы для карт разных эмитентов.

В базе данных может храниться несколько версий набора ключей Кас, Кс, Кі (до 256 версий). В базе хранятся мастер ключи EMV. При персонализации на карту записываются диверсифицированные на PAN индивидуальные ключи карты.

В ПЦ поддерживаются два способа диверсификации ключей, представленные в спецификациях EMV (Option A, Option B), см. *EMV Book 2: A1.4.2*.

Тип диверсификации ключа приложения EMV устанавливается при создании новой версии ключа.

На карте ведется счетчик выполненных операций с картой (ATC). Криптограммы карты формируются на диверсифицированных с помощью ATC индивидуальных ключах карты. Проверка и формирование криптограмм в ПЦ осуществляются внутри LSM.

Для on-line проверки ПИН, введенного клиентом, терминал посылает в ПЦ эквайера PIN блок, который эквайером в транзакциях авторизации или чтения баланса доводится до эмитента. Проверка ПИН осуществляется в ПЦ эмитента.

PIN блок формируется на основе PAN и введенного клиентом ПИН.

В базе данных ПЦ эквайера хранится базовый ключ шифрования PIN блоков (РЕК) для своих терминалов. В базе данных ПЦ эмитента, а хранится базовый ключ шифрования PIN блоков (РЕК) для непосредственно подключенных терминалов и внешних ПЦ. Может храниться несколько версий ключа РЕК.

PIN блок шифруется терминалом в соответствии с алгоритмом DUKPT, 3DES на ключе терминала, получаемый из базового ключа эквайера диверсификацией его на номере терминала.

Процессинговый центр эквайера перешифровывает PIN блок со своего ключа РЕК на диверсифицированный ключ РЕК эмитента. При межпроцессинговом обмене для шифрования PIN блоков используется алгоритм ZKA 3DES. Эмитент должен передать в ПЦ эквайера диверсифицированный ZKA 3DES ключ РЕК данного эквайера, получаемый из базового ключа эмитента диверсификацией его на номере ПЦ эквайера.

Ключ РРК в ПЦ эмитента служит для шифрования PIN блоков в базе данных эмитента. При on-line проверке PIN блок перешифровывается в LSM ПЦ эмитента с ключа РЕК на ключ РРК и зашифрованное на РРК значение сравнивается со значением PIN блока в базе данных эмитента.

«Чистые» карты, предназначенные для персонализации платежных карт, поступают в ПЦ в закрытом на лотовом ключе виде. Для персонализации новой карты необходимо предъявление этого ключа. Лотовый ключ передается в ПЦ поставщиком лота карт в зашифрованном на ключе КЕК виде. При загрузке в базу данных ключ перешифровывается с ключа КЕК на ключ LMK.

Ключи Кас, Кс, Кі, РЕК, РРК генерируются с помощью LSM непосредственно в ПЦ. При генерации ключей новой версии генерируются сразу все ключи Кас, Кс, Кі, РРК данной версии.

Все ключи (Кас, Кс, Ki, РЕК, РРК, лотовый ключ) хранятся в БД в зашифрованном на LMK виде.

Кроме симметричных 3 DES ключей в БД эмитента хранятся не симметричные RSA ключи, необходимые для персонализации платежных карт:

- Ключ эмитента (Issuer KEY);
- Ключ карты (Card Key).

Ключи (открытый и секретный) генерируются непосредственно в ПЦ с помощью LSM и записываются в базу. Секретный ключ хранится в зашифрованном на LMK виде.

Может быть сгенерировано несколько версий RSA ключей, используемых для персонализации разных платежных карт.

RSA ключи генерируются в целом для ПЦ, т.е. одни и те же ключи могут быть использованы для персонализации карт разных эмитентов.

Для RSA ключа эмитента должен быть получен и использован при персонализации платежных карт сертификат его открытого ключа на ключе СА (Центра сертификации). Обеспечиваются следующие возможности получения указанного сертификата:

- формирование сертификата непосредственно в ПЦ эмитента на рабочем месте оператора ПЦ в рамках собственного центра сертификации;
- формирование в виде файла запроса на сертификат во внешнюю подсистему СА и загрузка в базу ПЦ эмитента сертификата EMV, полученного от этой внешней подсистемы.

Структура файлов обмена с внешним СА соответствует документу *EMV CA. File Interface Formats. vers.6.0 Multos Ltd.*

Для обеспечения возможности динамической аутентификации платежных карт во все терминалы, подключенные к ПЦ, должен быть загружен открытый Certification Authority Key.

Все персонализируемые карты выпускаются для заданного AID - идентификатора приложения EMV на картах. В процессинговом центре обеспечивается возможность выпуска и обслуживания карт нескольких AID.

Для разных AID в ПЦ генерируются разные RSA ключи. Ключ СА генерируется для RID приложения EMV. RID содержит первые 5 байт AID.

В терминалы должны грузиться все актуальные версии открытого ключа СА всех ПЦ в системе для всех поддерживаемых в ПЦ RID.

Поддержка работы карт с разными AID (RID) обеспечивает возможность объединения ранее независимо развивающихся систем со своими ключами в единую систему с единым набором СА ключей.

Пул LSM

Среднее время проверки криптограммы платежной карты, поступившей в запросе терминала, в LSM порядка 200 миллисекунд.

Для повышения производительности системы обеспечивается возможность подключения к серверу обработки ПЦ нескольких LSM. При обработке транзакции или при выполнении каких-либо других криптографических операций сервером обработки выбирается первый свободный LSM в пуле. После завершения обработки LSM возвращается в пул свободных LSM.

Обмен с терминалами

Обмен между терминалами и ПЦ и между ПЦ эквайера и ПЦ эмитента может осуществляться по открытым TCP каналам или может быть защищен с помощью SSL.

Возможны два режима организации защиты с помощью SSL:

- без использования клиентских ключей терминалов;
- с использованием клиентских сертификатов и ключей терминалов.

Для реализации первого режима при обмене между терминалами и ПЦ в терминал должен быть загружен самоподписанный SSL сертификат СА ключа, на котором подписан ключ сервера обработки ПЦ.

Для реализации второго режима в терминал, кроме того, должен быть загружен SSL ключ терминала. У каждого терминала должен быть свой ключ терминала. В SSL сертификате открытого ключа терминала параметр Common Name должен иметь значение идентификатора терминала в системе.

При установлении SSL соединения с терминалом сервер обработки проверяет, что идентификатор терминала, от которого поступил запрос, совпадает со значением параметра Common Name сертификата открытого ключа терминала.

В сервер обработки в обоих режимах грузятся:

- SSL сертификат СА;
- SSL сертификат ключа сервера обработки, подписанный в СА, и секретный ключ сервера обработки.

В обоих режимах обеспечивается шифрование сообщений обмена между сервером обработки и терминалом.

В первом режиме обеспечивается аутентификация сервера обработки терминалом. Во втором режиме обеспечивается также аутентификация терминала сервером обработки ПЦ.

Для обеспечения защиты обмена между ПЦ эквайера и ПЦ эмитента в сервер обработки ПЦ эквайера должен быть загружен SSL сертификат СА эмитента. В качестве клиентского ключа при межпроцессинговом обмене используется ключ сервера обработки ПЦ эквайера.

Сертификаты и ключи генерируются вне ПЦ. Обеспечивается лишь загрузка их в хранилище сертификатов сервера обработки и использование их при установлении соединения с терминалами или между ПЦ.

Ключ после загрузки не может быть экспортирован из хранилища. При загрузке ключ и сертификат должны представляться в формате PEM или P12 в зашифрованном на пароле виде. Пароль предъявляется только один раз - при загрузке. При использовании ключей и сертификатов предъявление пароля не требуется.

Система реализована таким образом, чтобы обеспечивалась возможность смены ключей терминалов, ключа сервера и сертификата СА при необходимости.

Разграничение доступа к информации и контроль работы операторов

В ПЦ доступ к информации базы данных имеют следующие типы пользователей:

- операторы;
- администраторы.

Администраторы имеют полный доступ к информации всех эмитентов системы, а также к информации, передаваемой внешним ПЦ.

Администратор системы имеет также права на:

- создание новых операторов и контроль их работы;
- подключение новых эмитентов и терминалов к системе;
- блокировку работы эмитентов и внешних ПЦ;

- генерацию новых версий ключей Кас, Кс, Ki, РЕК, РРК, Certification Authority Key, Issuer Key, Card Key.
- загрузку лотового ключа в базу данных;
- создание карт персонализации;
- создание типов платежных карт;
- загрузку SSL сертификатов защиты обмена с терминалами;
- настройку функционирования системы.

Операторы для каждого эмитента могут иметь следующие права:

- контроль;
- персонализация;
- управление.

Полномочие *контроль* обеспечивает только чтение данных по данному эмитенту.

Полномочие *персонализация* обеспечивает чтение данных по данному эмитенту и формирование заявок на персонализацию новых карт для существующих клиентов, создание новых клиентов.

Полномочие *управление* дает права изменения данных по клиентам данного эмитента, в том числе изменения количества средств на счетах клиентов, права создания нового клиента, формирования заявок на персонализацию новых карт для существующих клиентов данного эмитента.

Операторы могут иметь разные права по доступу к информации разных эмитентов.

Операторы могут иметь также полномочие доступа к *Подсистеме эквайера*.

Если данное полномочие установлено, то оператору предоставляется возможность просмотра всей зарегистрированной информации по внешним ПЦ.

Все действия операторов, в том числе вход и выход из системы регистрируется в ПЦ.

Вход в рабочие места ПЦ осуществляется только при предъявлении пароля.

Структура программных и технических средств процессингового центра

Процессинговый центр включает в себя:

- SQL сервер с базой данных системы;
- сервер обработки процессингового центра с пулом LSM;
- рабочее место оператора ПЦ;
- рабочее место администратора LSM;
- рабочее место персонализации платежных карт.

Сервер обработки ПЦ

В процессинговом центре может быть один или несколько серверов обработки, выполняющих разный набор функций. На одном компьютере может быть установлен только один сервер обработки. Сервер обработки представляет собой Windows службу. Настройка и управление данной службой осуществляется программой *Управления сервером обработки*, устанавливаемой на компьютере вместе со службой сервера обработки.

Сервер обработки может выполнять следующий набор функций:

- обработку транзакций, поступающих от терминалов и обмен информацией с внешними ПЦ;
- формирование файлов обработанных транзакций для передачи эмитентам;

- разгрузку архивов и журналов и сборку мусора в БД;
- загрузку файлов эмитентов с заявками на создание новых клиентов системы, с лимитами эмитентов и т.д.;
- подготовку файлов заявок персонализации карт;

Несколько серверов обработки одновременно могут выполнять обработку транзакций, поступающих от терминалов. Все остальные функции должны выполняться только одним сервером обработки. Настройки сервера обработки хранятся в базе данных, что позволяет контролировать ограничения на совокупное использование серверов обработки в ПЦ. Настройки могут быть просмотрены на рабочем месте оператора.

Сервер обработки периодически записывает в базу данных свое состояние (*Я жив*), включающее в себя состав работающих подсистем состав работающих LSM. На рабочем месте оператора администратор системы может просмотреть состав работающих серверов обработки.

Сервер обработки может посылать по e-mail отчеты о своем состоянии внешним абонентам. Высылается информация:

- о запуске и останове сервера обработки;
- о изменении состава работающих подсистем;
- о изменении количества работающих LSM в пуле;
- о выполнении разгрузки архива;
- об ошибках при формировании выходных файлов сервером и обработке входных файлов и заявок персонализации.

Рабочее место оператора ПЦ

Рабочее место оператора ПЦ обеспечивает выполнение следующих функций:

- контроль функционирования системы;
- просмотр и корректировку количества средств на счете клиента;
- просмотр и корректировку средств учтенных в лимитах клиентов;
- блокировку/разблокировку карт/счетов клиентов, эмитентов в целом, внешних ПЦ;
- просмотр журнала операций со счетом;
- просмотр архива транзакций;
- формирование заявок на выпуск новых платежных карт;
- создание новых клиентов и редактирование атрибутов существующих;
- ввод новых лимитов и ограничений на покупаемые товары;
- корректировку справочников курсов валют;
- создание рекламных сообщений;
- формирование расписания выгрузки отчетов для эмитентов в виде xml файлов;
- создание новых операторов системы и контроль их работы;
- подключение новых эмитентов, терминалов и внешних ПЦ к системе;
- генерацию новых версий ключей Кас, Кс, Ki, РЕК, РРК, Certification Authority Key, Issuer Key, Card Key;
- загрузку лотового ключа в базу данных;
- создание карт персонализации;
- создание типов платежных карт;
- настройку функционирования системы.

В ПЦ может быть развернуто несколько рабочих мест операторов. Рабочее место, на котором будут выпускаться или корректироваться карты персонализации и осуществляться загрузка лотового ключа в БД, должно быть оснащено устройством чтения карт.

Рабочее место администратора LSM

Рабочее место администратора LSM обеспечивает:

- ввод/удаление ключа LMK на карту LSM или карту персонализации;
- ввод/удаление ключей КЕК на карту LSM или карту персонализации;
- безопасное копирование ключей с одной карты LSM (карты персонализации) на другую.

Ввод ключа LMK или КЕК в LSM осуществляется, как ввод трех “чистых” компонент. Рабочее место администратора LSM –автономно и не имеет доступа к БД системы.

Рабочее место персонализации платежных карт

Рабочее место персонализации обеспечивает персонализацию платежных карт.

Рабочее место должно быть оснащено двумя устройствами чтения карт.

В одно устройство должна быть вставлена карта персонализации. В другое устройство вставляется персонализируемая платежная карта.

Карты могут выпускаться в ручном режиме, когда оператор сам выбирает заявку, по которой осуществляется персонализация или полуавтоматическом режиме, когда при наличии заявок выпуск очередной карты осуществляется сразу после ее установки.

Время персонализации карты – порядка 15 секунд.

Рабочее место персонализации –автономно и не имеет доступа к БД системы.

Требования к среде функционирования ПЦ

Данные ПЦ хранятся в базе данных. В качестве СУБД системы должен использоваться Microsoft SQL Server 2012 или выше. SQL Server должен работать под управлением операционной системы Windows Server 2008 или выше.

Сервер обработки должен функционировать под управлением операционной системы Windows Server 2008 или выше.

Все рабочие места должны функционировать под управлением операционной системы Windows 8 или выше.