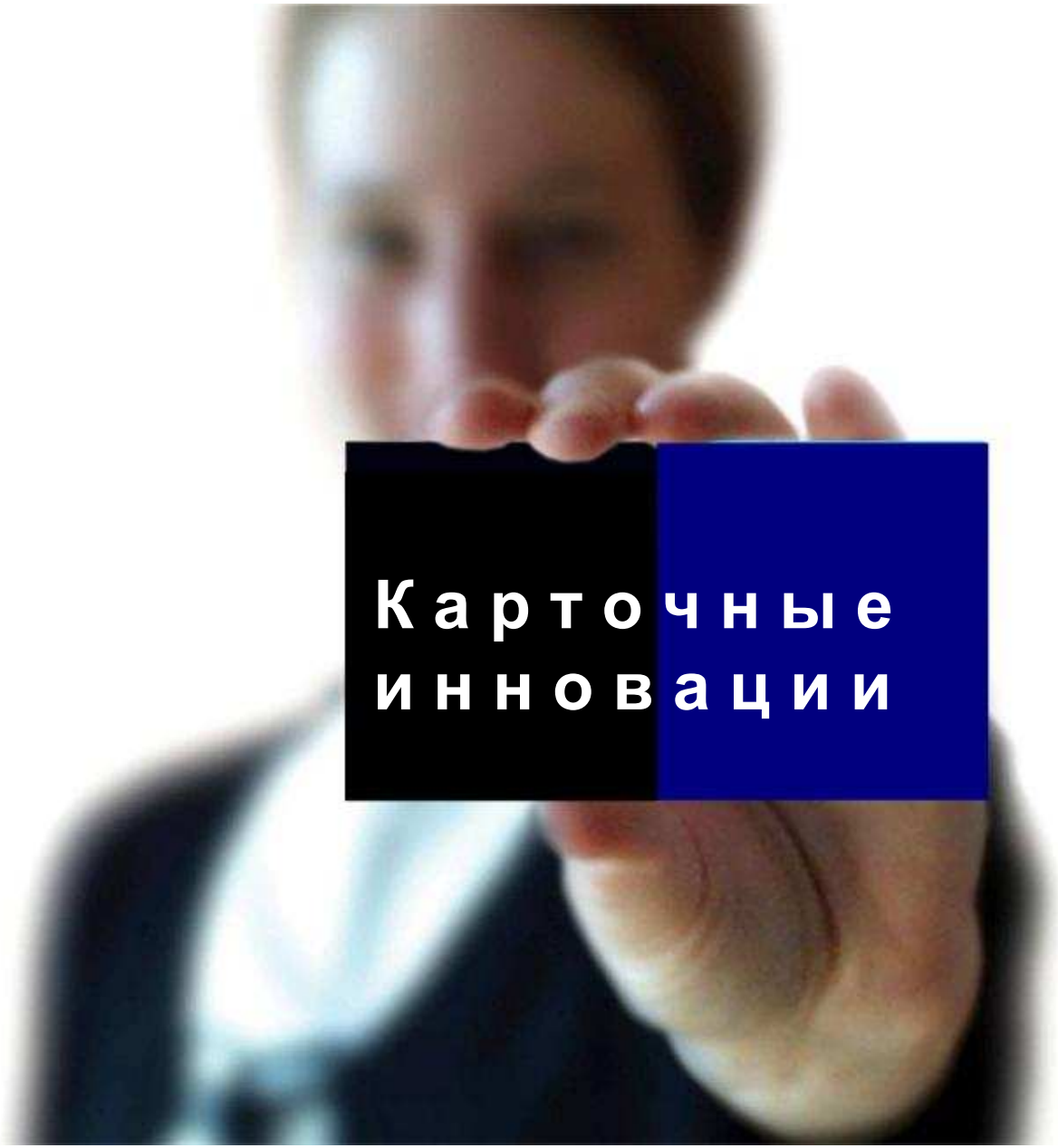
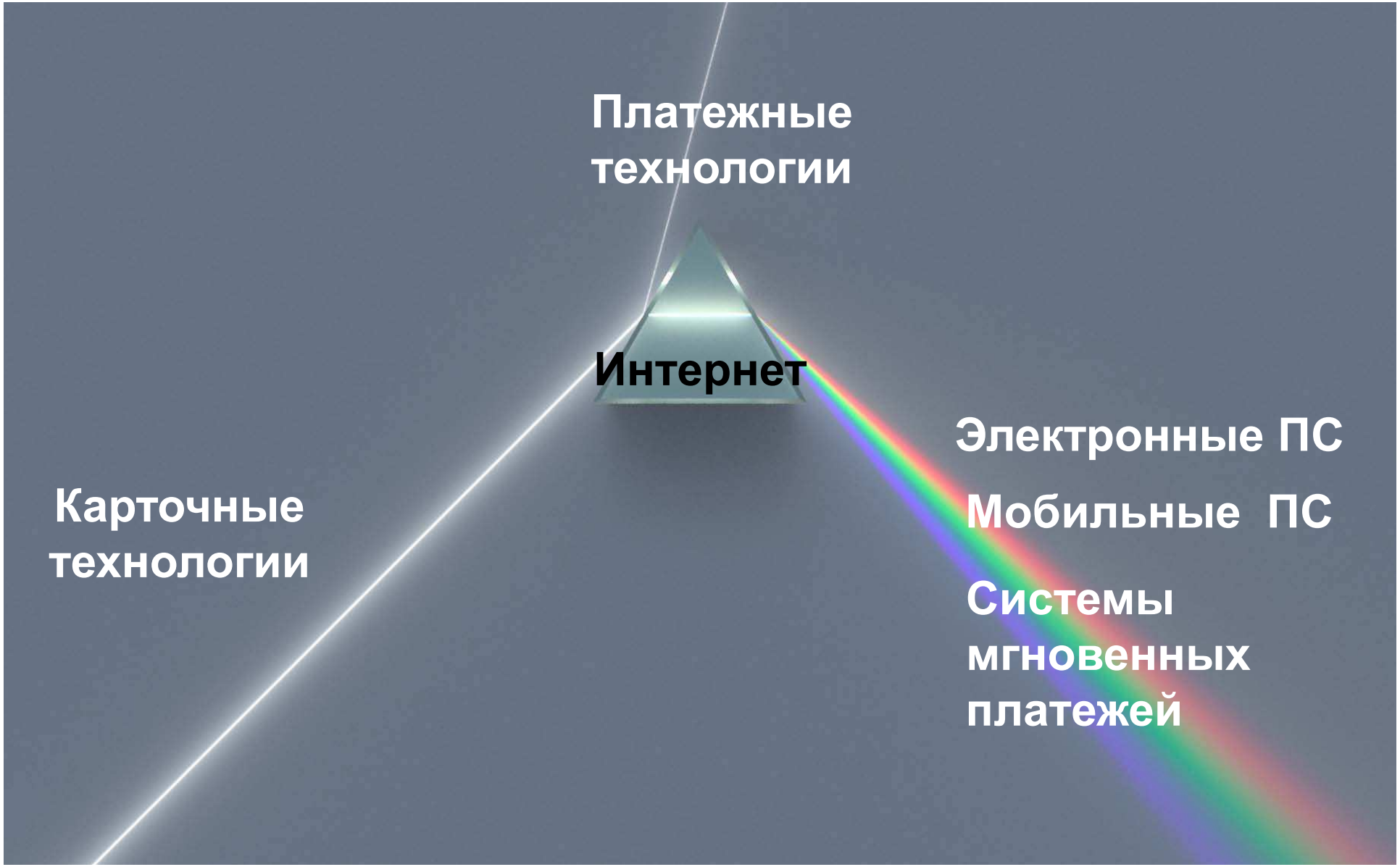


Группа компаний ITNT и холдинг Платежные технологии

Банковские карты

Весь путь развития банковских карт – это путь борьбы за безопасность платежей и адаптацию к современному развитию технологий.



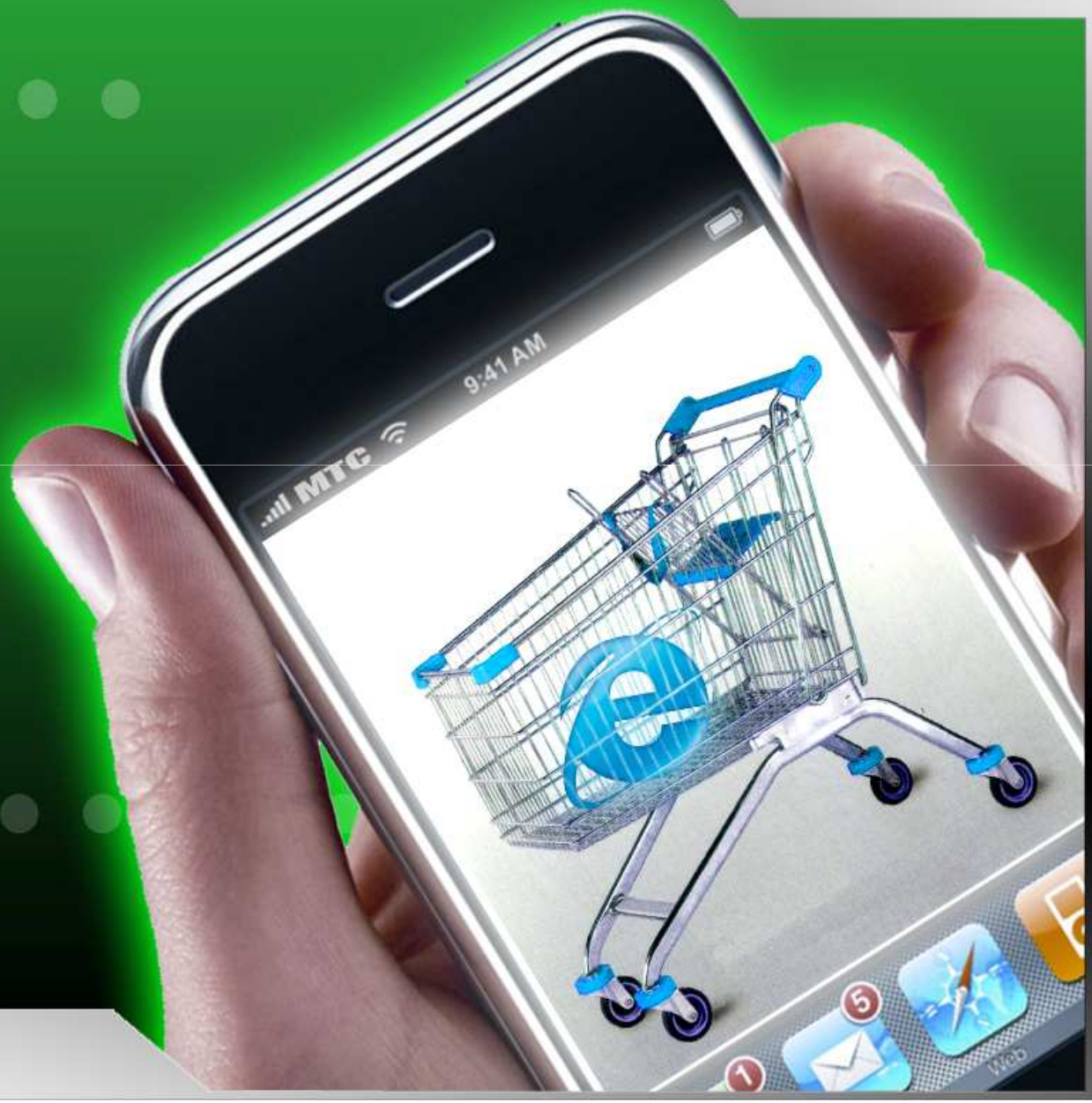
2007 г – 0,3%

2011 г. – 3%

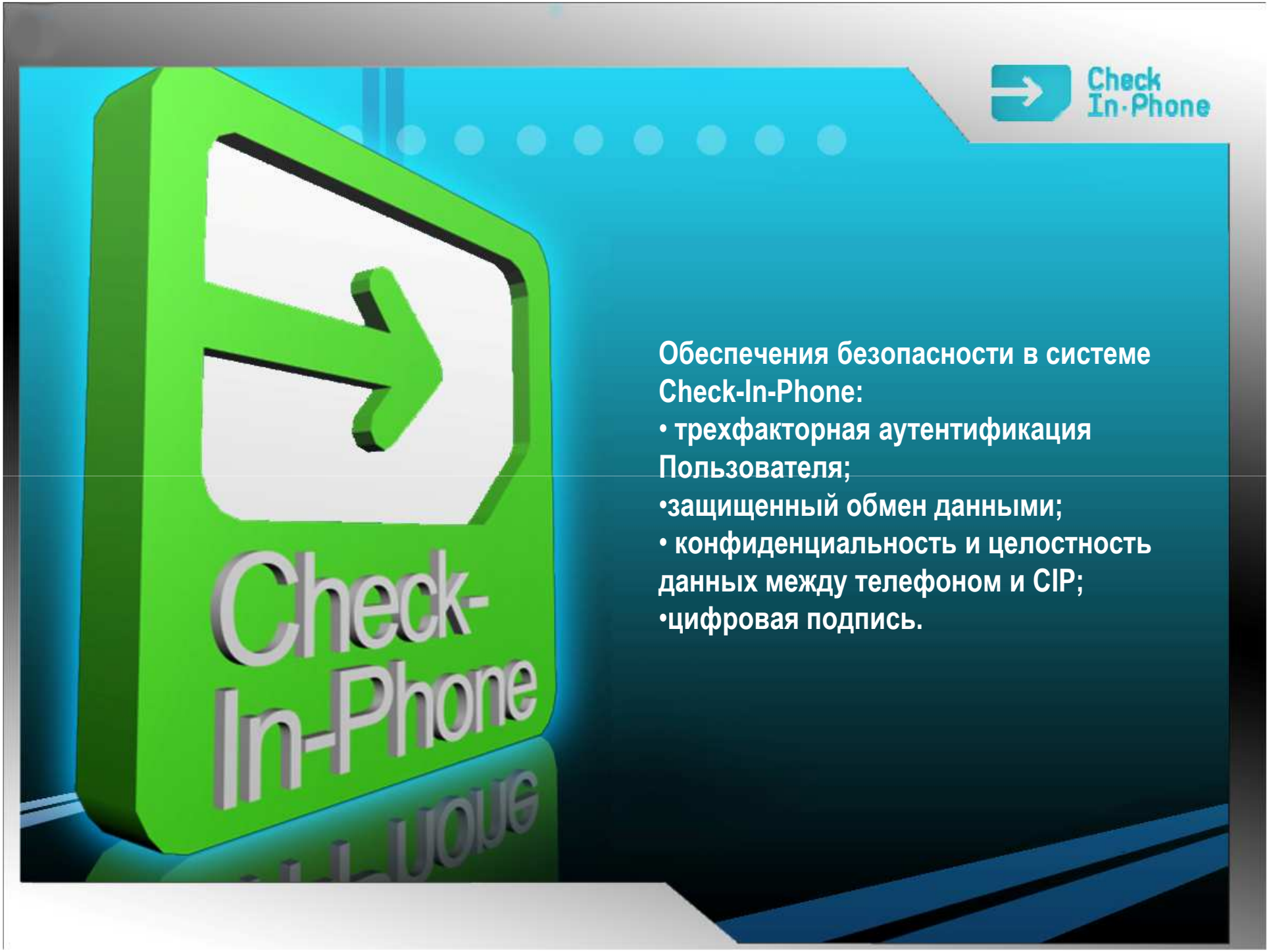
2014 г. – 30%?

Check In·Phone

Мобильный телефон - это единственный инструмент, который может заменить самую совершенную банковскую карту!




Check
In·Phone
Check-
In-Phone
Check-In-Phone - это возможность создать индивидуальный набор дистанционных сервисов для Пользователей на основе мобильного телефона



Обеспечения безопасности в системе Check-In-Phone:

• трехфакторная аутентификация Пользователя;

•защищенный обмен данными;

• конфиденциальность и целостность данных между телефоном и CIP;

•цифровая подпись.

Мобильное приложение

Check-In-Phone - это надежное стандартное средство подтверждения подлинности Пользователя Check-In-Phone перед Партнером для персонифицированного получения услуг.

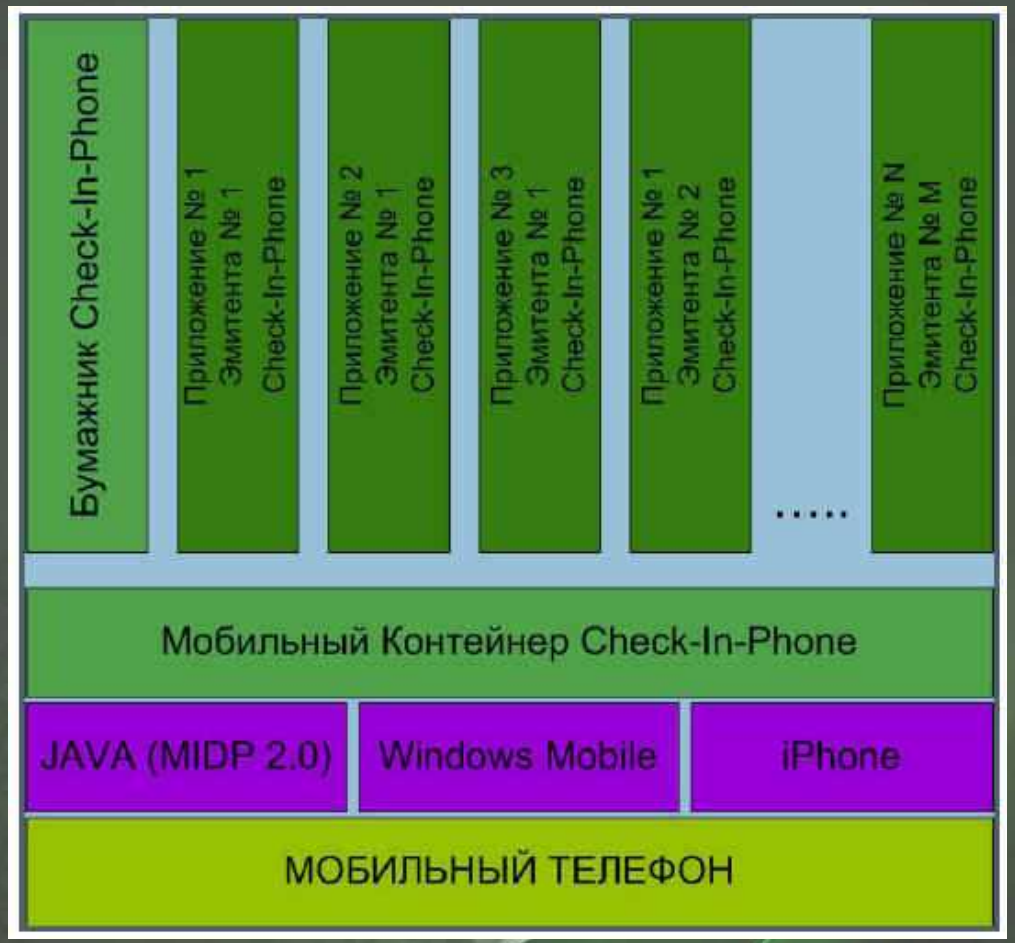
В основе технологии мобильного приложения Check-in-Phone лежит протокол аутентификации Пользователя MasterCard Mobile Authentication (MMA).

Мобильное приложение позволяет осуществить автоматическую многофакторную авторизацию: пользователя, терминала, приложения, банковской карты.

Архитектура

Мобильный Контейнер Check-In-Phone, является фактически фундаментом, ядром, на платформе которого реализуются бумажник и другие приложения.

Основным элементом Контейнера является элемент безопасности который должен поддерживать стандарты GlobalPlatform и иметь возможность управления через платформу TSM (Trusted Service Manager).



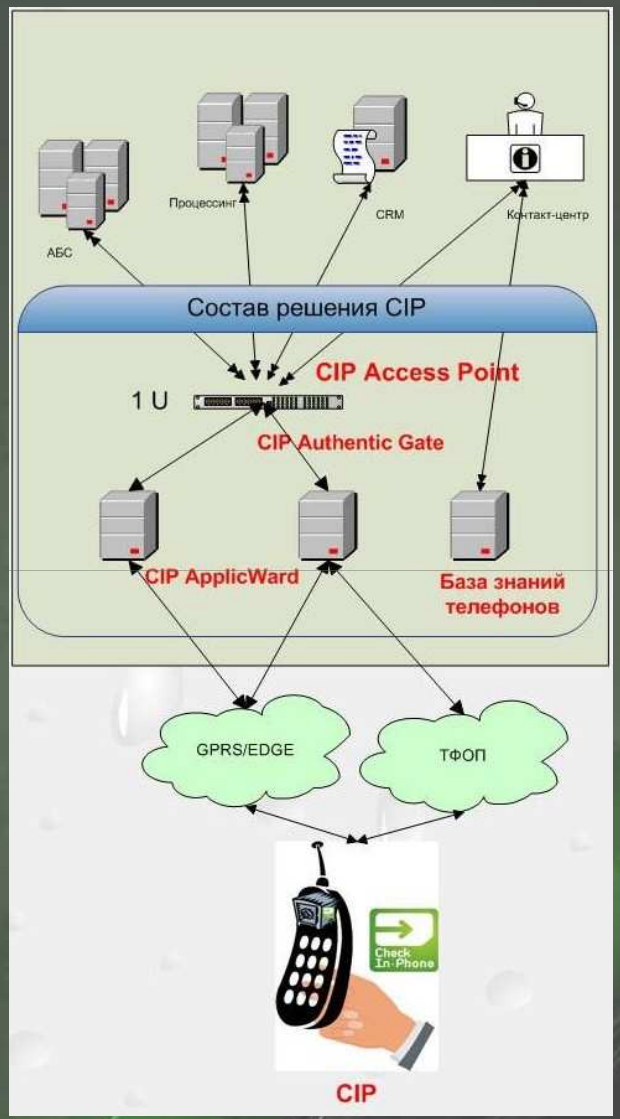
В структуре Мобильного приложения (как надстройки над Мобильным Контейнером) присутствует данные для его идентификации, ключевые и секретные данные, URL системы аутентификации Check-In-Phone, глобальные переменные, CIPML код бумажника (его разметка), признак языка интерфейса, CAP профайл.

В системе Check-In-Phone не хранятся никакие сведения о Пользователях (Персональные данные) Приложений. Вместо реальных реквизитов Пользователей (например, номера карты) применяются их заменители (например, хэш-функции номера карты или иные идентификаторы клиента).

Преобразование идентификаторов в реальные реквизиты в системы банка (например, в номер карты) выполняется в CIP AP на стороне Банка.

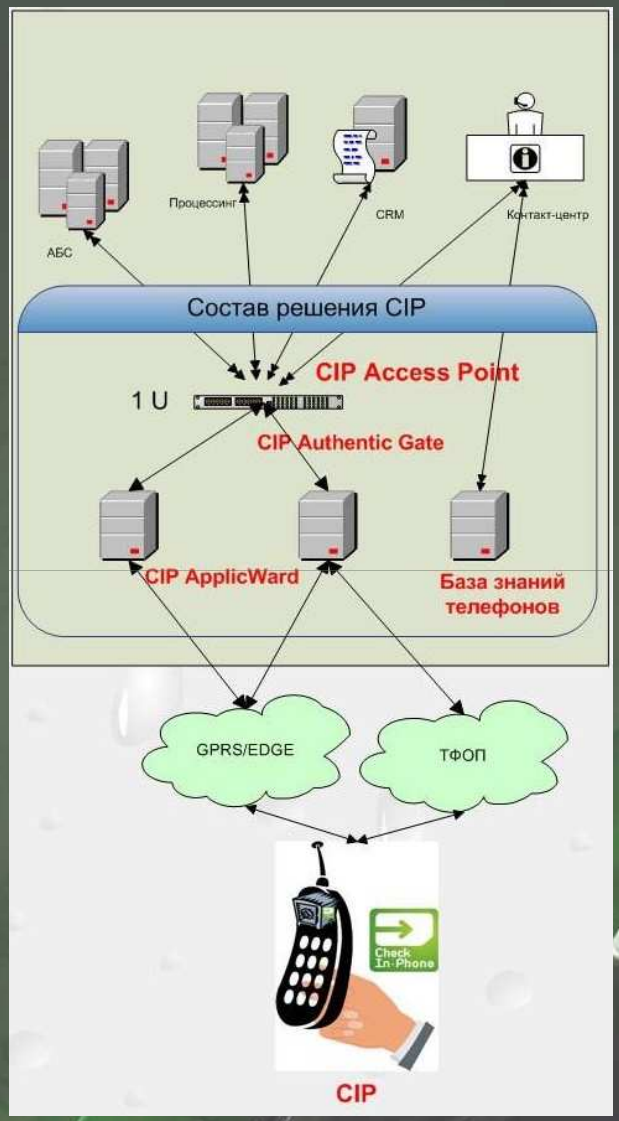
Состав серверных решений:
• серверная подсистема системы CIP - Authentic Gate (AG).
• серверная подсистема CIP ApplicWard (AW).
• серверная подсистема шлюза – CIP Access Point (AP)

Серверная подсистема Check-In-Phone AG взаимодействует с Check-In-Phone на мобильном телефоне по протоколу HTTPS.



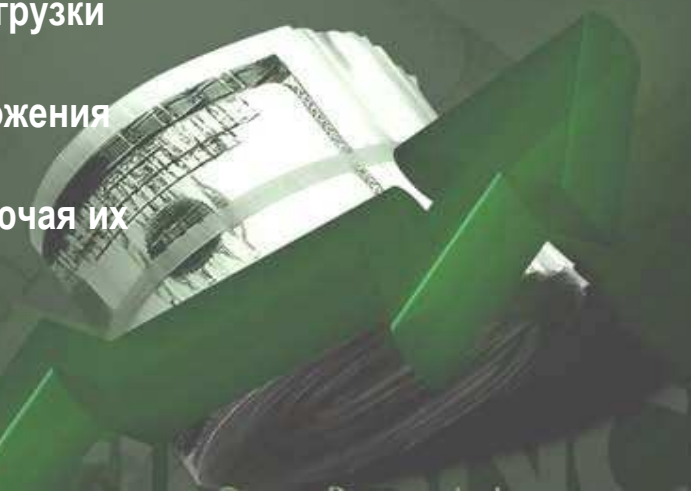
Все входящие запросы отправляются на обработку на CIP AG серверной подсистемы Front-Office. CIP AG выполняет необходимые операции.

Для обработки запроса Пользователя CIP AG связывается с информационной системой Организатора через CIP AP, являющегося Эмитентом данного Приложения.



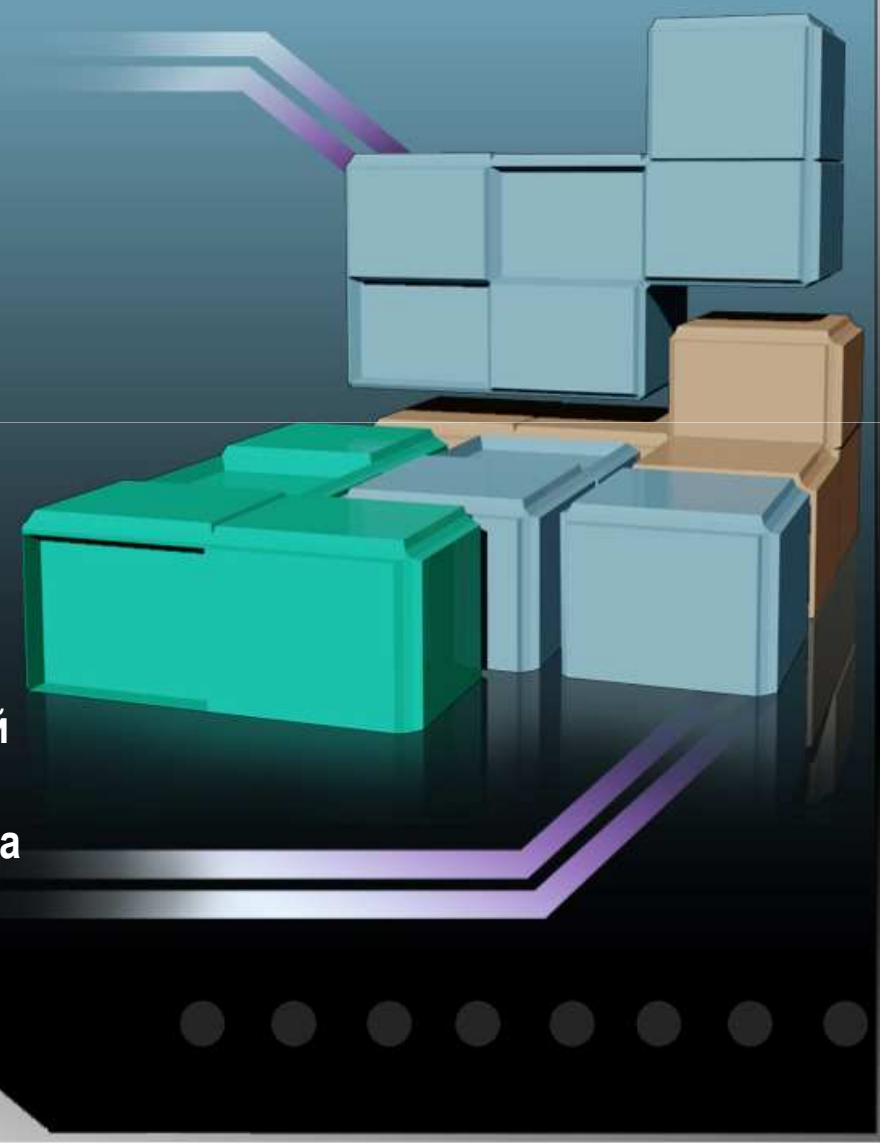
Особый статус приложения Бумажник заключается в том, что это приложение загружается на телефон вторым (сразу после загрузки Мобильного Контейнера Check-In-Phone) и в дальнейшем используется:

- Организации безопасной загрузки Приложения Check-In-Phone;
- Активации Приложения;
- Удаление Приложения;
- Восстановления персонализационных данных Приложений;
- Организации удобного клиентского интерфейса для работы с Приложениями Check-In-Phone (в частности, получение списка доступных приложений эмитента и выбор приложения для загрузки на телефон);
- Организации защищенного канала передачи данных от Приложения Check-In-Phone к его Эмитенту;
- Управления Пользователями Приложениями Эмитентов, включая их блокировку и удаление.



Инсталляция

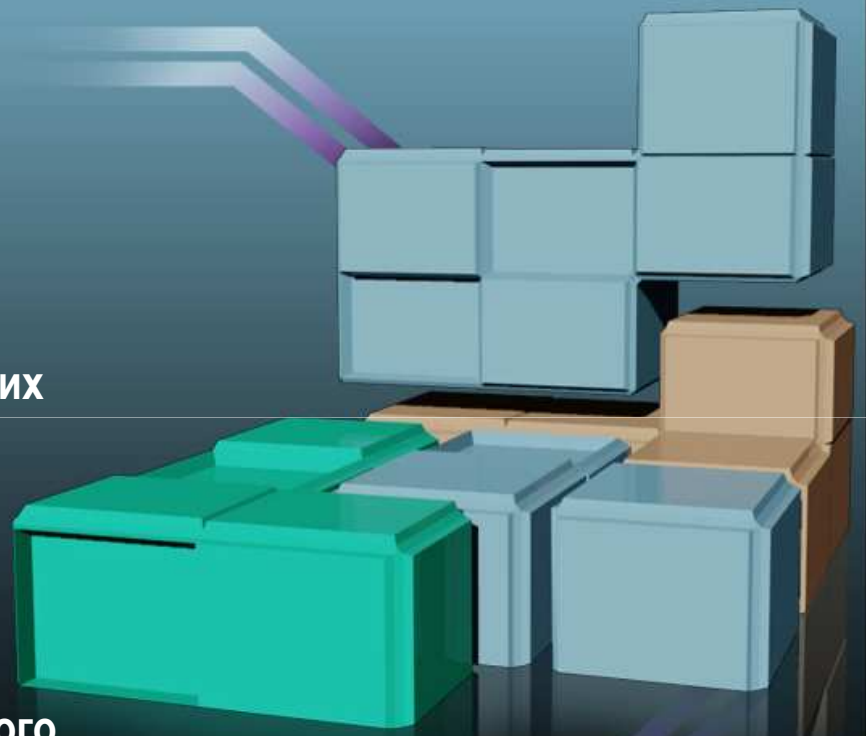
Результатом инсталляции является:
• получение клиентом уникальных идентификаторов в системе ”Check-In-Phone” для приложения “бумажник” и приложения эмитента;
• установка PIN-кодов приложений для генерации разовых паролей и аутентификации клиента;
• обеспечения клиента возможностью обмениваться чувствительной информацией с системой эмитента;
• загрузка на мобильный телефон клиента персональных сервисных меню приложений для обеспечения клиента возможностью пользоваться базовыми сервисами эмитента и устанавливать новые сервисы



Check In-Phone

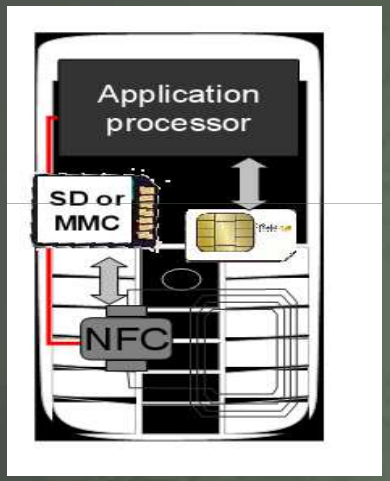
Безопасность

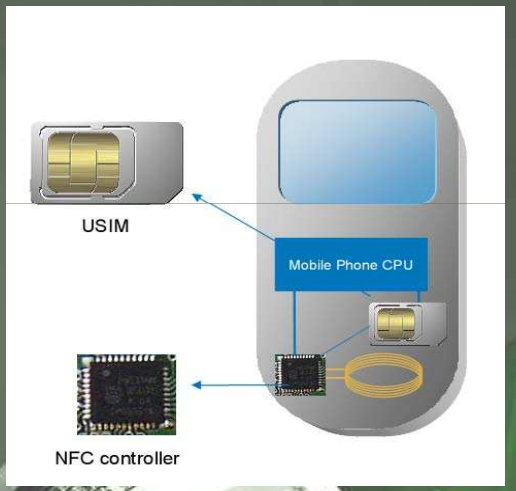
Атаки злоумышленников (например,перехват значения одноразовых паролей при уже известном мошенникам значении зашифрованного ключа Customer Master Key, загрузка вирусов-шпионов на сотовый телефон Пользователя, сканирующих значения ПИН-кода и ключа Customer Master Key) позволяет потенциальному мошеннику похитить лишь отдельные секреты трехфакторной схемы аутентификации. Получить доступ ко всем секретам одновременно очень сложно и главное - дорого.



Элемент безопасности

Элемент безопасности может быть реализован с использованием различных технологий: на отдельной микро-карте, на Sim-карте мобильного оператора или с использованием специальных телефонов или стикеров.
Использование технологии NFC предпочтительно, поскольку, совместима с пассивными бесконтактными технологиями и позволяет в дальнейшем использовать приложения на созданной сети NFC.





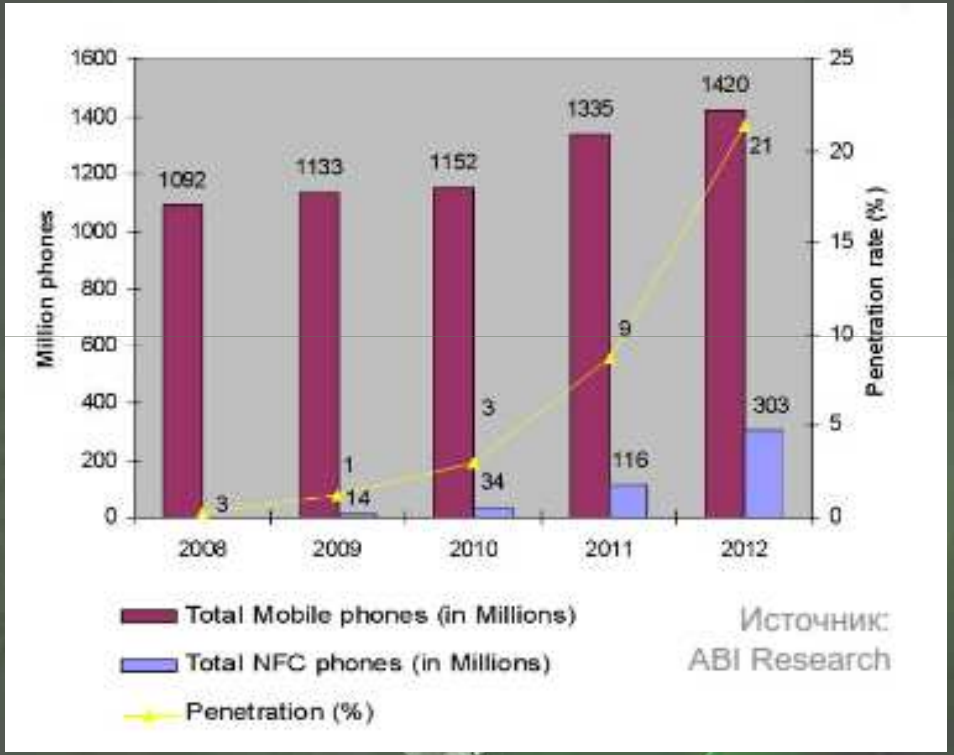
Элемент безопасности интегрирован в телефон в виде отдельного конструктивного элемента

Элемент безопасности интегрирован в съемный элемент (memory card)

Элемент безопасности реализован в SIM карте телефона

Предпосылки и перспективы массового внедрения мобильных приложений на основе NFC

- Успех проекта Felica Mobile (более 50 млн. телефонов NTT DoCoMo оснащены NFC интерфейсом , 250 тыс. ридеров)
- Положительный опыт пилотных проектов в Европе
- Распространенность совместимых бесконтактных технологий и подготовленность населения
- Заинтересованность операторов в новых видах услуг
- Наличие стандартов
- Увеличение производства NFC телефонов



Преобладающие мобильные NFC сервисы – транспортные и платежные

Check In·Phone

Check-In-Phone – это возможность для создания индивидуальных наборов дистанционных сервисов для широкого спектра систем.

Последние системные разработки:

- **транспортный кошелек Сбербанка;**
- **универсальная электронная карта;**
- **система M-pay.**

ООО «Мобильные решения»
www. paytech.ru

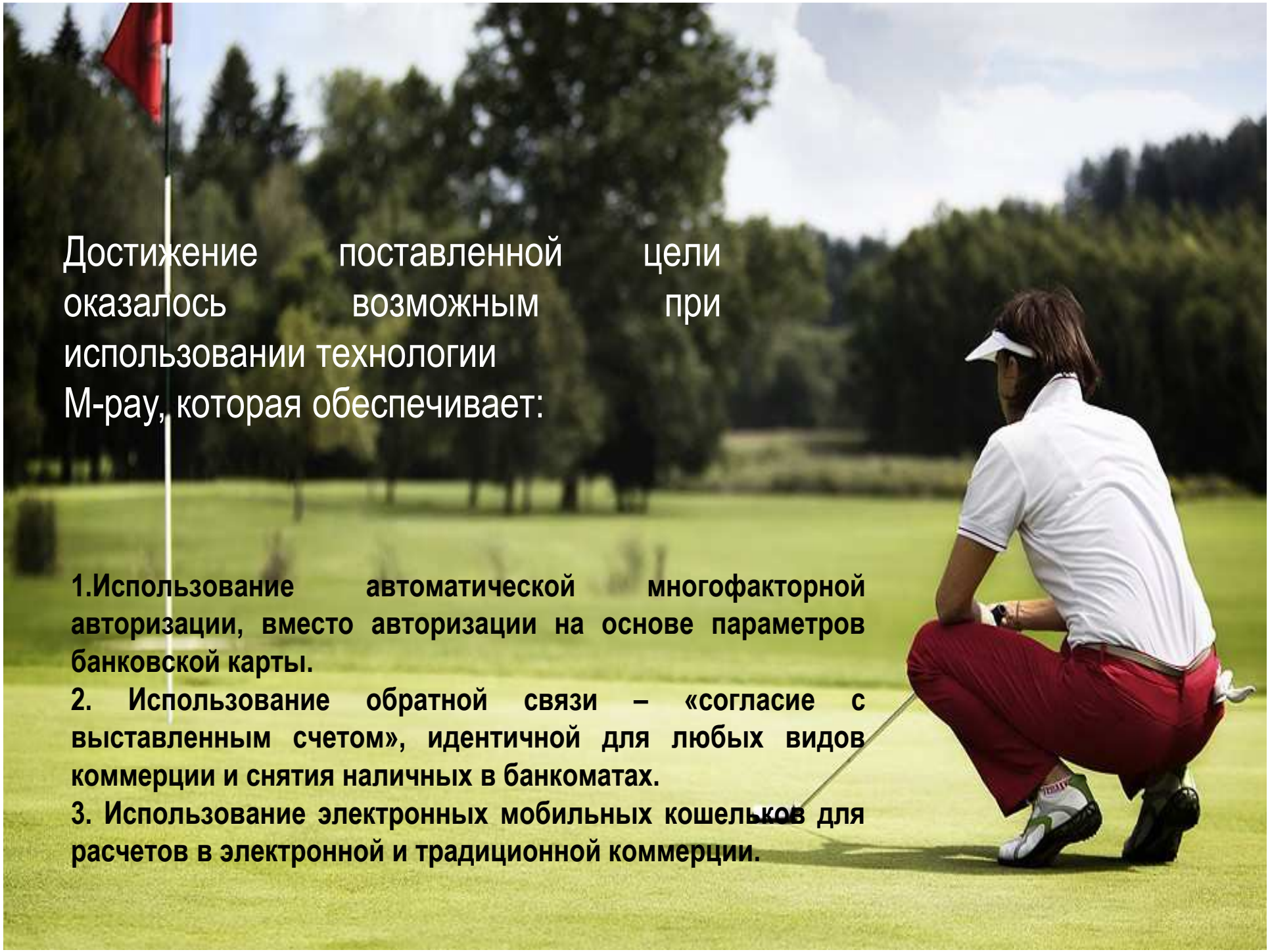
Группа компаний ITNT и холдинг Платежные технологии

Цель : создание банковского продукта

1. В полной мере использующего существующие сети эмиссии и эквайринга

2. Имеющего функциональность банковской карты и продуктов электронных платежных систем

3. Обеспечивающего максимальную безопасность платежей для всех видов коммерции едиными не стандартными средствами



Достижение поставленной цели оказалось возможным при использовании технологии M-pay, которая обеспечивает:

1.Использование автоматической многофакторной авторизации, вместо авторизации на основе параметров банковской карты.

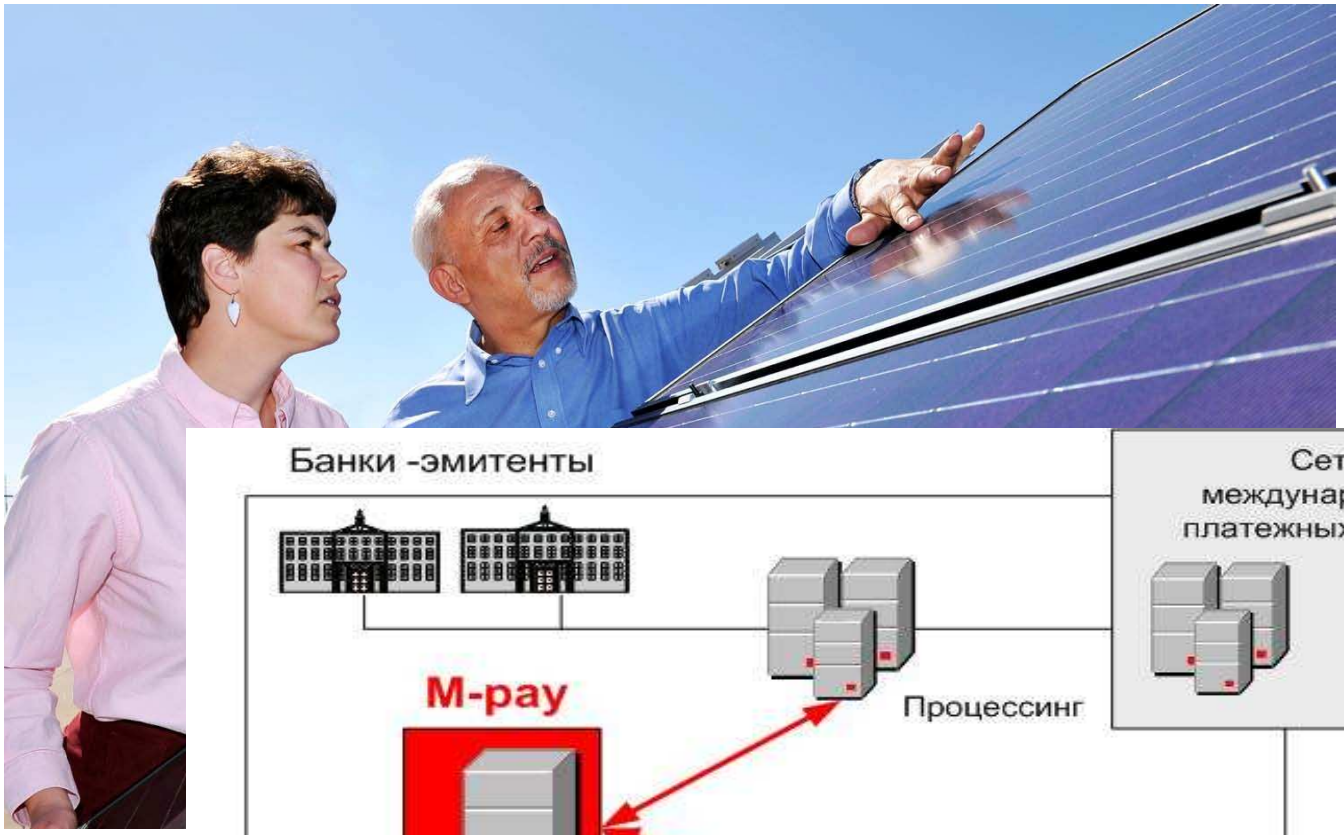
2. Использование обратной связи – «согласие с выставленным счетом», идентичной для любых видов коммерции и снятия наличных в банкоматах.

3. Использование электронных мобильных кошельков для расчетов в электронной и традиционной коммерции.

Мы назвали этот продукт Универсальная мобильная карта (Universal Mobile Card – UMC)

На первом этапе UMC представляет собой обычную банковскую карту и мобильный терминал с инсталлированным на нем защищенным мобильным приложением (по технологии Check-in-Pone)

На втором этапе – только мобильное приложение.


Банки -эмитенты
Сеть
международных
платежных систем
M-pay
Процессинг
Электронные
кошельки
Эквайер
Эквайер
Эквайер
Клиент
Бескон-
тактные
автоматы
Магазины
с NFC
Банкоматы
Магазины,
рестораны
Интернет
магазины

Основные принципы реализации технологии M-pay на первом этапе:

1. Клиент открывает в банке UMC, получает банковскую карту, которая регистрируется как мобильная.
2. Скачивает, инсталлирует и регистрирует мобильное приложение.
3. Устанавливает режимы и лимиты платежей.
4. Организует электронные кошельки.
5. Производит платежи:

а) активизируя на заданное время мобильное приложение,

в) направляя по интернет или USSD согласие с ближайшим выставленным счетом (многофакторная авторизация),

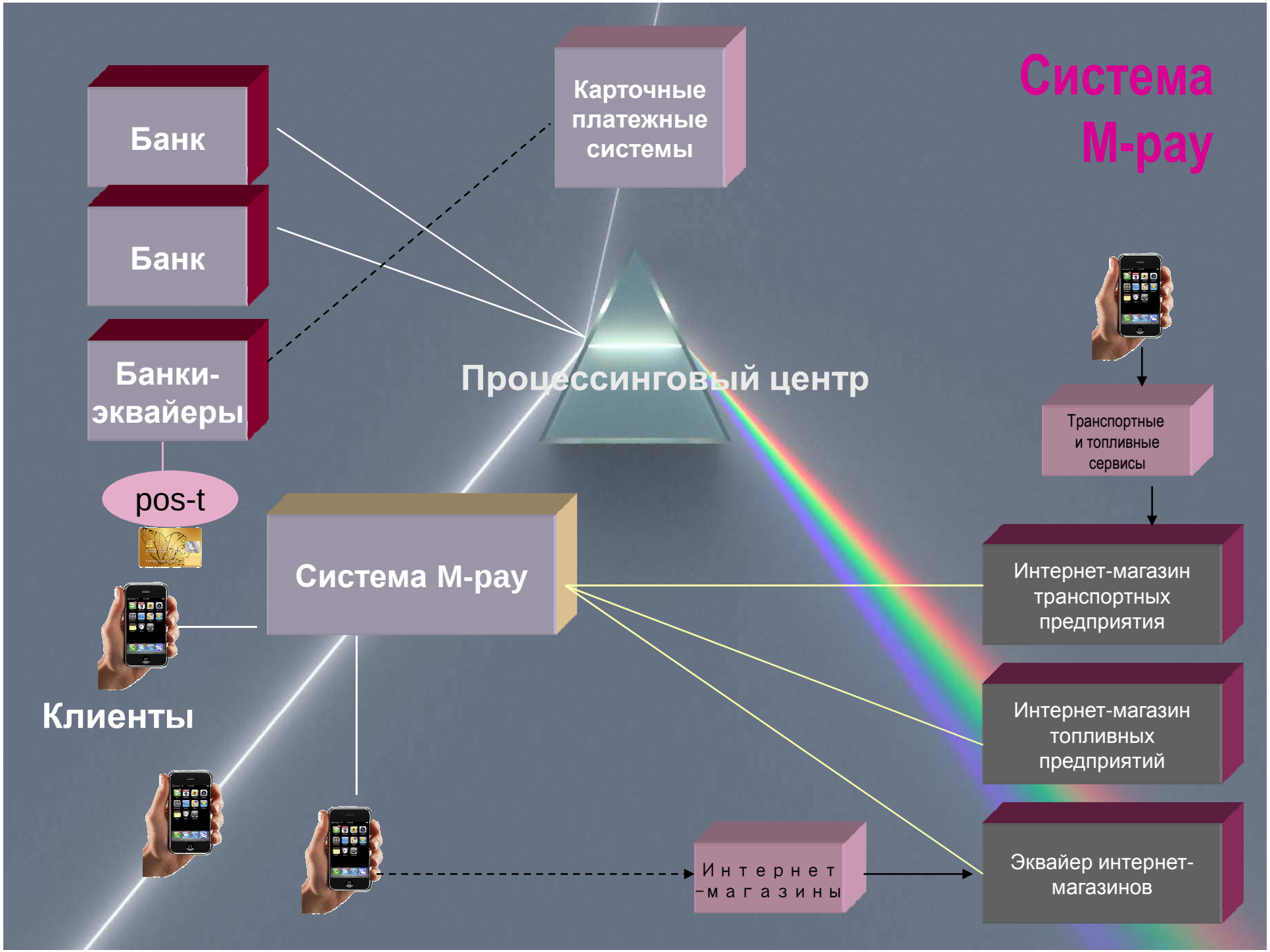
с) производит платеж по карте (снимает наличные) стандартными способами.

6. Пополняет электронные кошельки.
7. Производит платежи через электронные кошельки («пассивные» или «активные» NFC)

Основные принципы реализации технологии M-pay на втором этапе:

1. Вместо обычной банковской карты – получает виртуальную, которая регистрируется как «мобильная».
2. При осуществлении платежей в электронной коммерции параметры карты не вводятся в ручную, а осуществляется многофакторная авторизация UMC.
3. При расчетах в традиционной коммерции используются терминалы NFC и электронные кошельки.

Технология M-pay защищена патентами


Система
M-pay
Банк
Банк
Банки-
эквайеры
Карточные
платежные
системы
Процессинговый центр
pos-t
Система M-pay
Клиенты
Транспортные
и топливные
сервисы
Интернет-магазин
транспортных
предприятия
Интернет-магазин
топливных
предприятий
Эквайер интернет-
магазинов
Интернет
-магазины

Продуктовая линейка

Сервисы оплаты

- банковский бумажник;
- электронный кошелек;
- транспортный кошелек;
- топливная карта.

Сервисы технологии

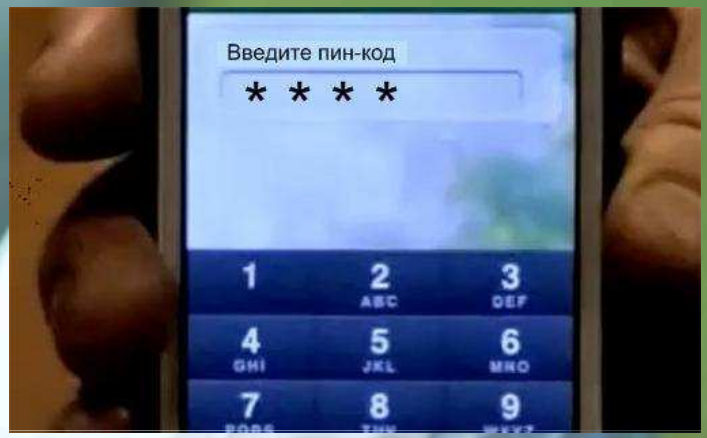
- настройка автоматического согласия: по сумме, по времени, по месту, по назначению платежа;
- настройка автоматического согласия при отсутствии связи в месте оплаты.
- подтверждение согласия с оплатой счета после его выставления;

Универсальные сервисы

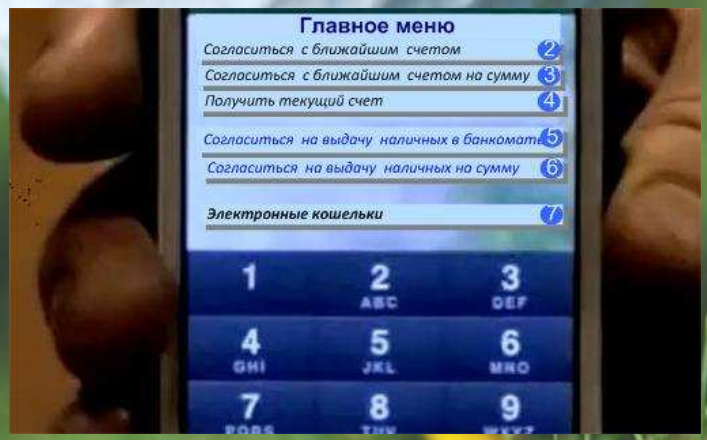
- авторизация без ввода параметров;
- мгновенные платежи;
- микроплатежи.

Пример работы UMC на первом этапе

Для активации M-pay необходимо ввести код активации (пин-код)

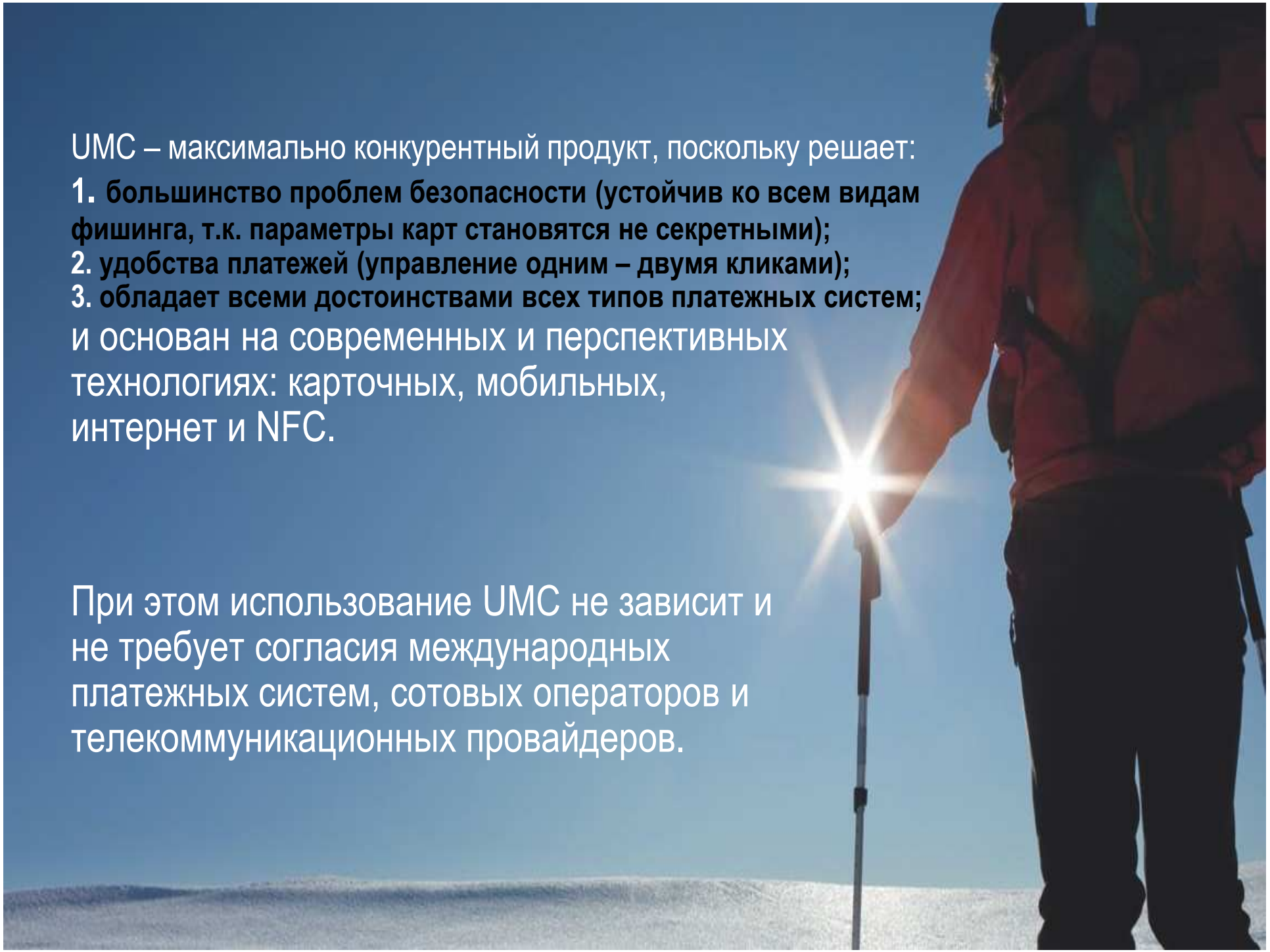


Приложение может оставаться активным в течение заданного времени. Интервал времени задается в меню настроек



Пример работы UMC на первом этапе

Перед авторизацией «мобильной» банковской карты для любых видов коммерции и снятия наличных , производится активизация UMC и выбор типа «согласия». После чего производится оплата.

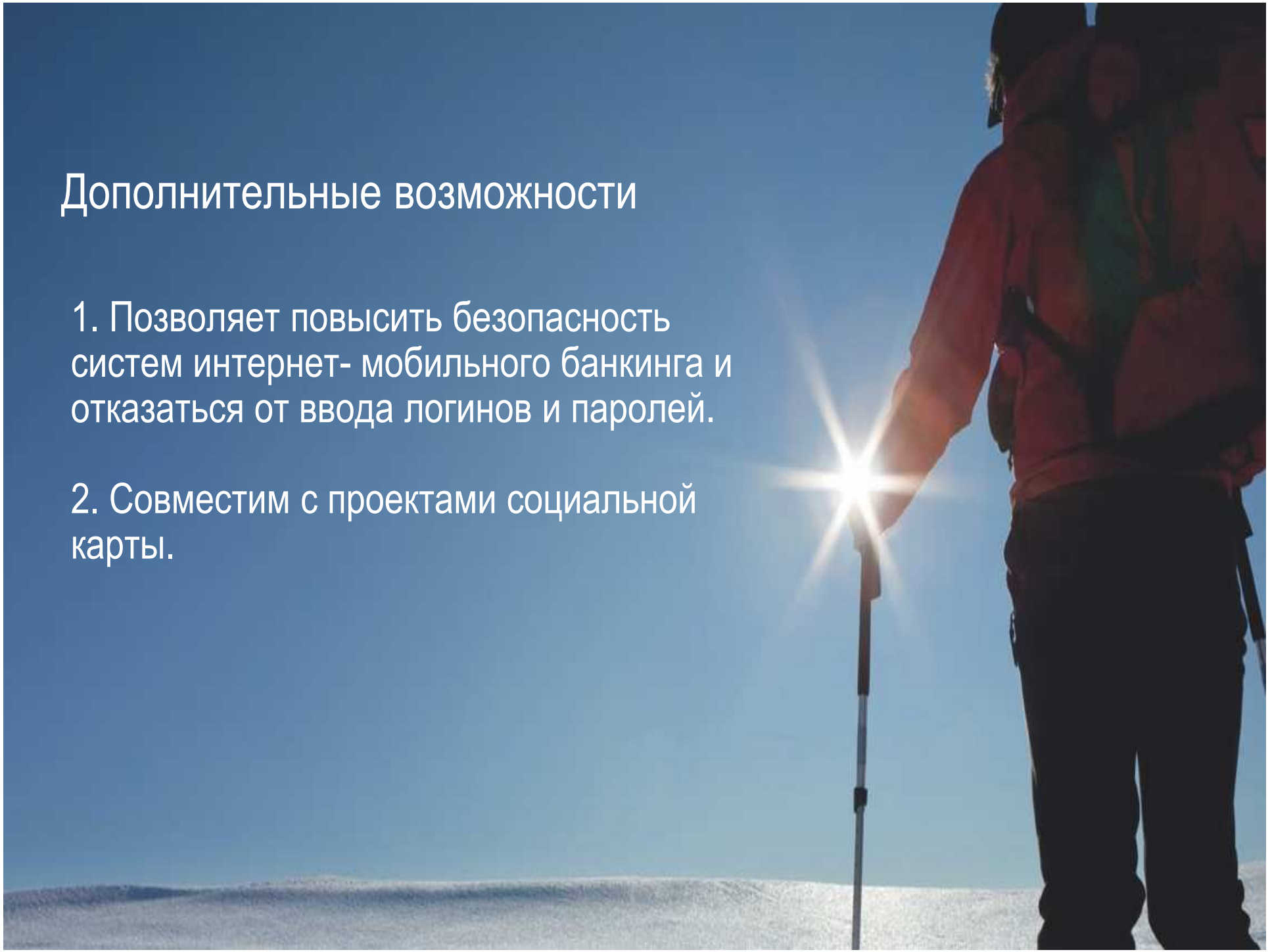


UMC – максимально конкурентный продукт, поскольку решает:

1. большинство проблем безопасности (устойчив ко всем видам фишинга, т.к. параметры карт становятся не секретными);
2. удобства платежей (управление одним – двумя кликами);
3. обладает всеми достоинствами всех типов платежных систем;

и основан на современных и перспективных технологиях: карточных, мобильных, интернет и NFC.

При этом использование UMC не зависит и не требует согласия международных платежных систем, сотовых операторов и телекоммуникационных провайдеров.

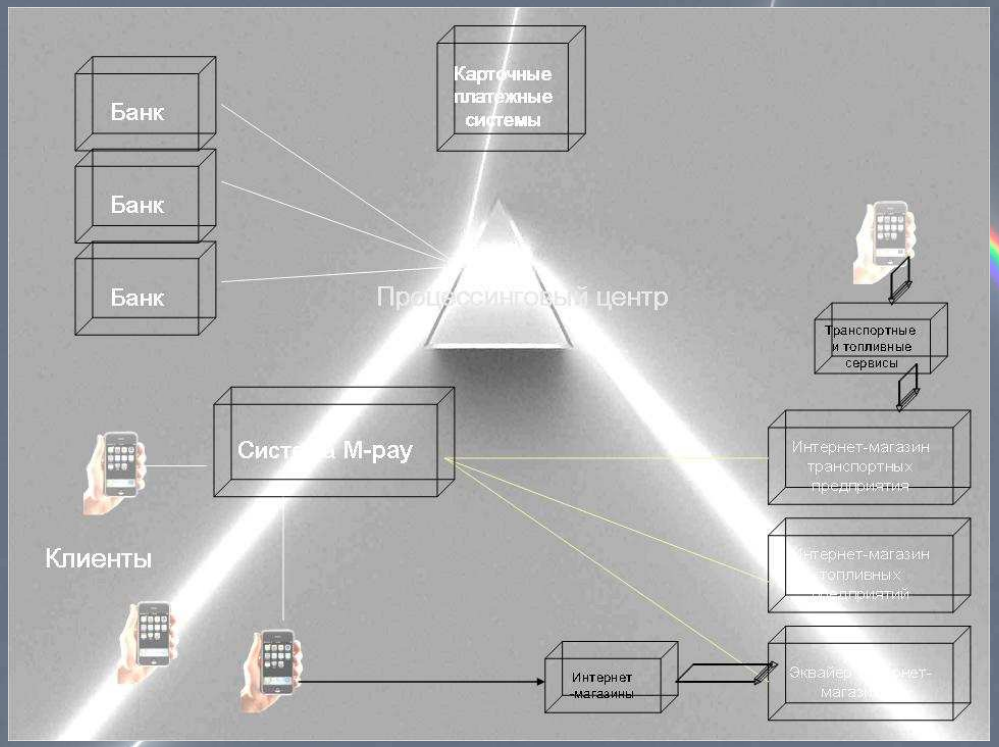


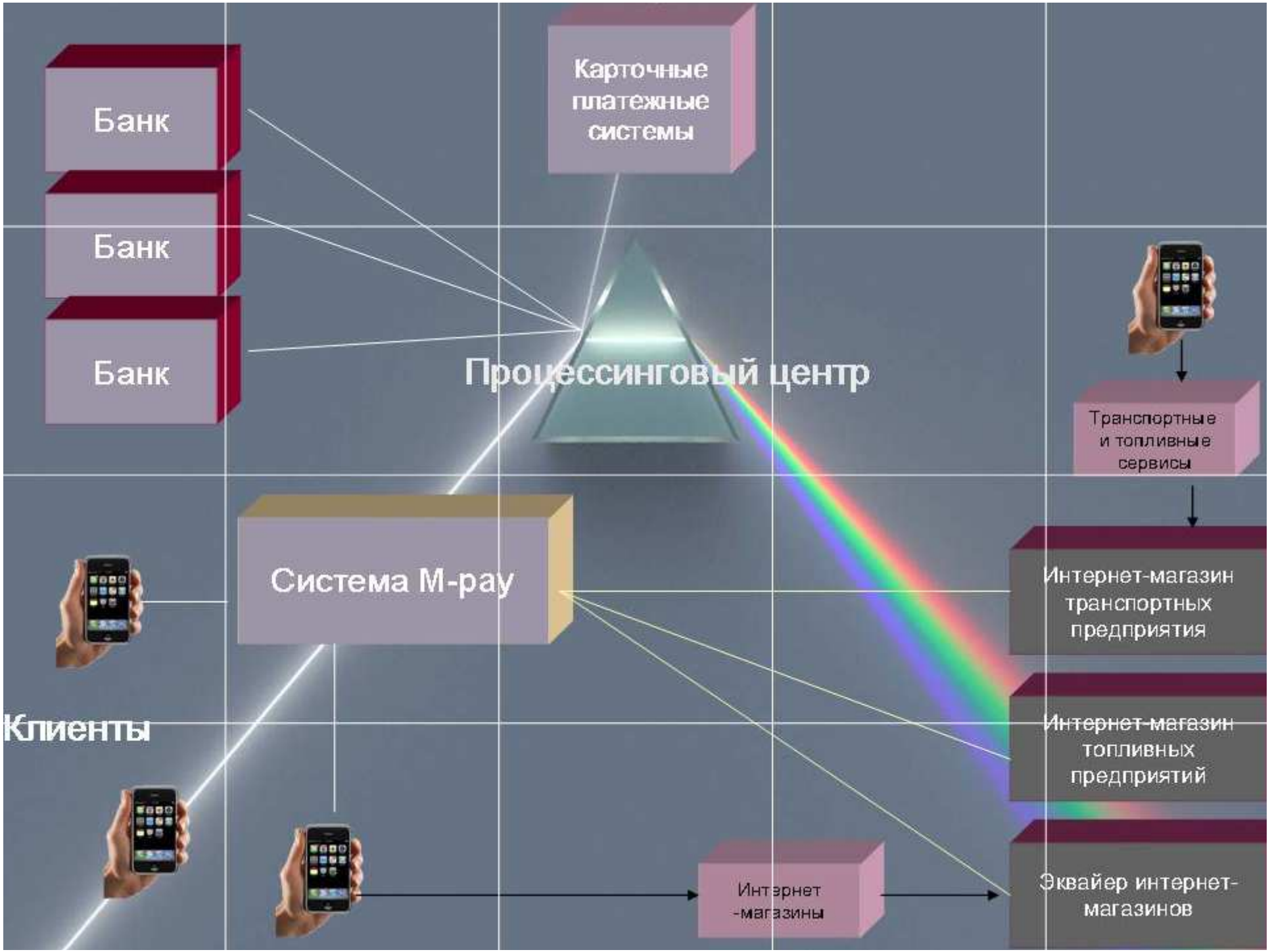
Дополнительные возможности

1. Позволяет повысить безопасность систем интернет- мобильного банкинга и отказаться от ввода логинов и паролей.

2. Совместим с проектами социальной карты.

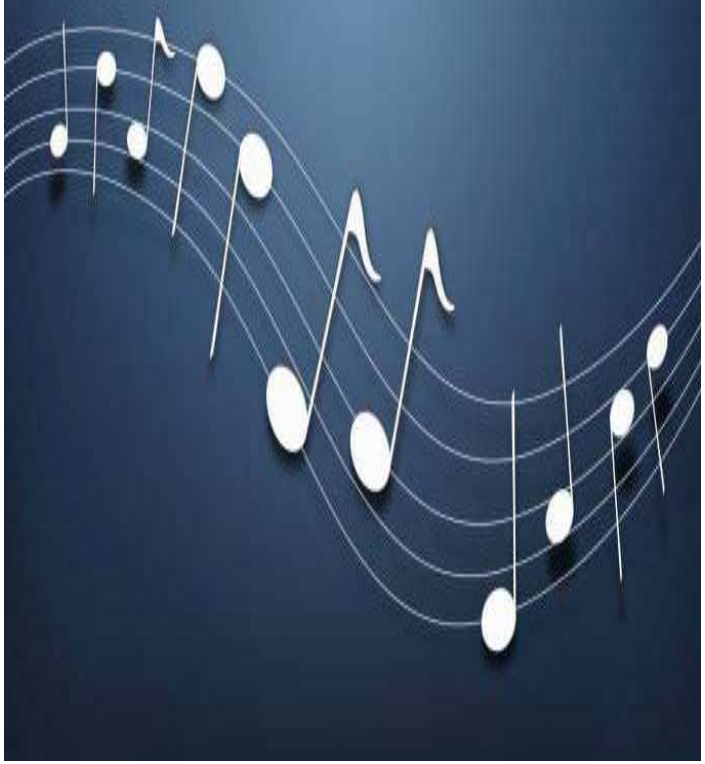
Готовность проекта – 90%

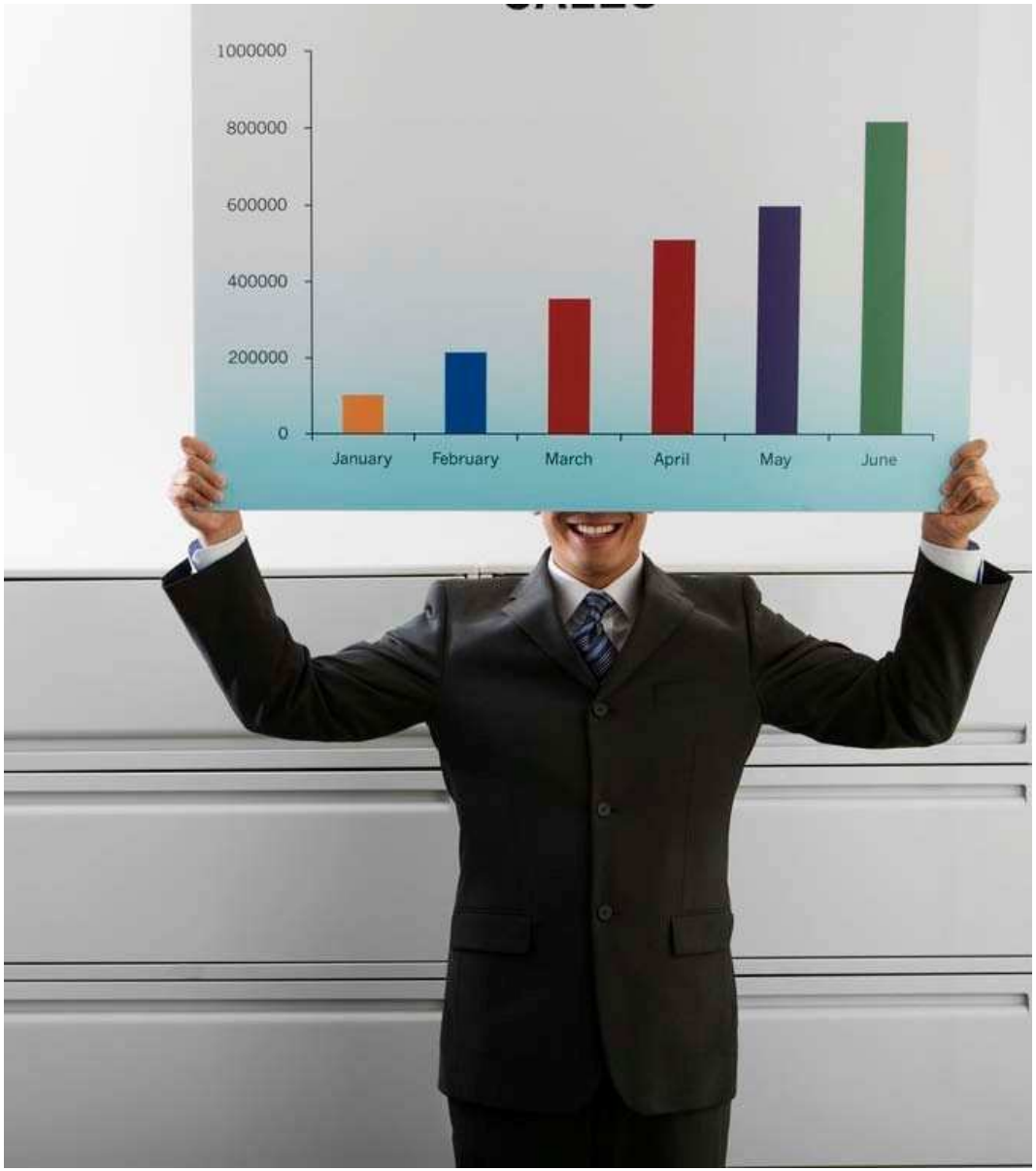



Банк
Банк
Банк
Карточные платежные системы
Процессинговый центр
Транспортные и топливные сервисы
Система M-pay
Интернет-магазин транспортных предприятия
Интернет-магазин топливных предприятий
Клиенты
Интернет -магазины
Эквайер интернет-магазинов

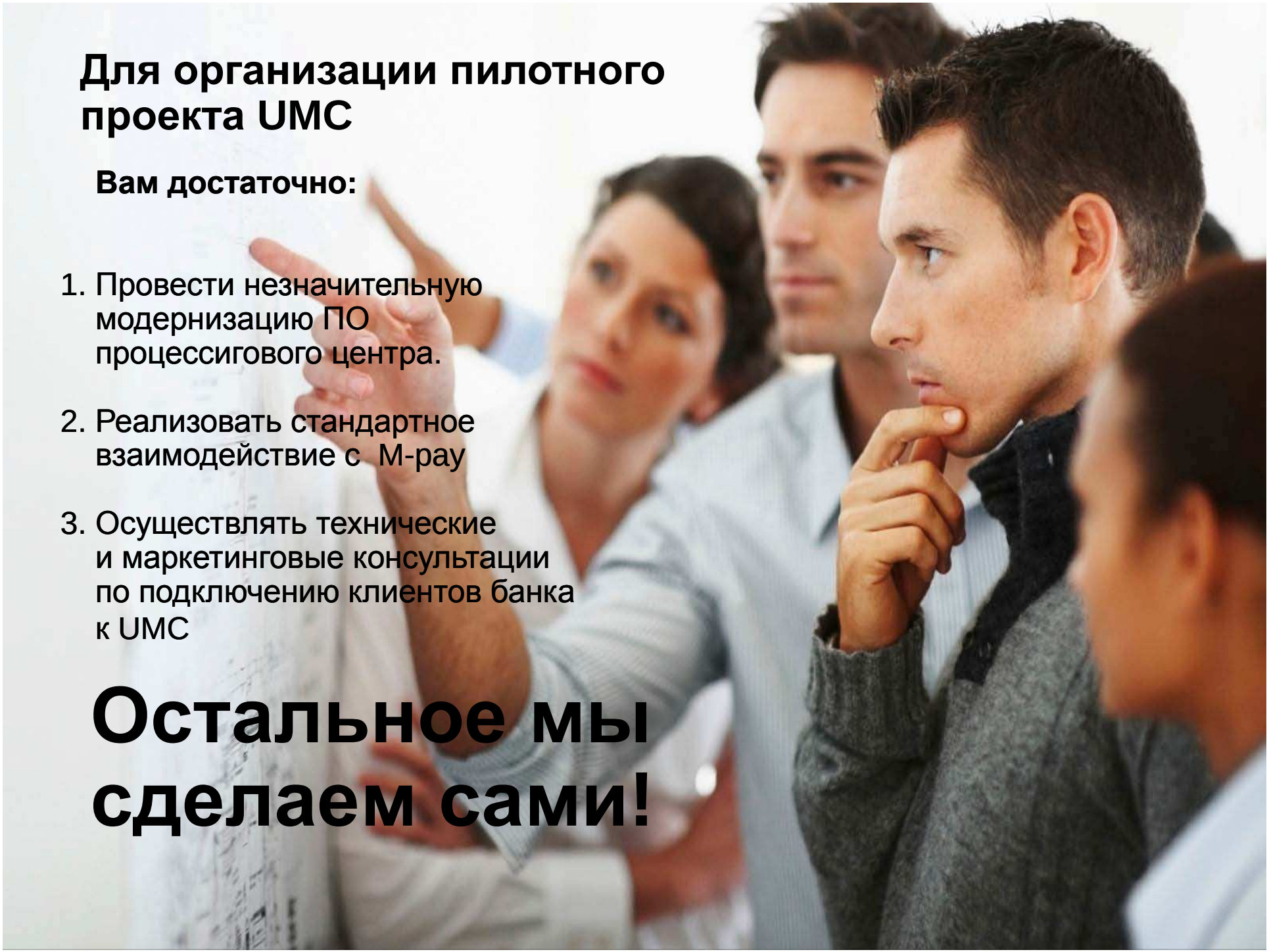
Планируемые показатели

Пилотный проект – 1 год
1 миллион UMC – 2 года
Доход – 1,5 миллиарда рублей






Примерьте
на себя
UMC !
Более подробная информация на сайте umc.unipaid.ru
Связаться с нами можно: info@unipaid.ru



Для организации пилотного проекта UMC

Вам достаточно:

1. Провести незначительную модернизацию ПО процессигового центра.
2. Реализовать стандартное взаимодействие с M-pay
3. Осуществлять технические и маркетинговые консультации по подключению клиентов банка к UMC

Остальное мы сделаем сами!


Спасибо за внимание!