НСПК

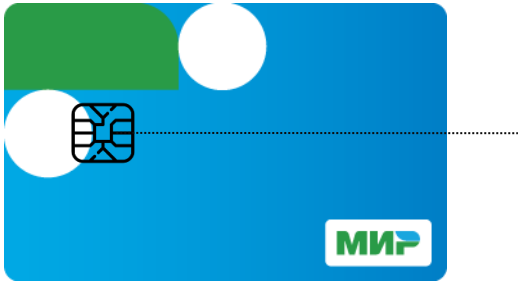
Безопасность карты «Мир»

Российская
платежная система

МИР

Голдовский Игорь Михайлович
Главный архитектор
АО «НСПК»

Приложение «Мир»



Контактное

Бесконтактное

Мобильное

Контактное приложение «Мир»

Основные характеристики контактного приложения «Мир»

- **Полностью соответствует стандарту EMV 4.3 и поддерживает базовые функции EMV-приложения, включая ODA, целостность критичных статических данных приложения, онлайновую взаимную аутентификацию приложения карты и эмитента, защищенный скрипт-процессинг, проверку PIN на карте**
- **Принимается в любом действующем терминале EMV L1&L2**
- **Поддерживает Global PIN**
- **Персонализация приложения не зависит от модели микроконтроллера карты (приложение поддерживает стандартизованный и широко применяемый в индустрии механизм CPS 1.1)**

Контактное приложение «Мир»

Основные преимущества контактного приложения «Мир»

- **Выбор профиля обработки транзакции в зависимости от параметров транзакции (размер, валюта, тип транзакции), терминала/магазина (terminal type, additional terminal capabilities и т.п.) и карты (бесконтактный/контактный интерфейс)**

- **Расширенные процедуры управления рисками (дополнительные проверки определенных условий, увеличенное количество счетчиков и способов их использования в зависимости от выбранного профиля обработки транзакции, циклические счетчики, MTA, Max offline Days)**

- **Дополнительная non-EMV-функциональность**

Бесконтактное приложение «Мир»

Основные характеристики бесконтактного приложения «Мир»

- **Реализуется в рамках версии 1.1 апплета (MPA 1.1)**
- **Наследует основные свойства контактного приложения, включая выбор профиля обработки транзакции, объекты данных и команды**
- **Суммарное время обработки операции на терминале и карте – менее 400 мс**
- **Может использоваться для оплаты проезда на транспорте в форме:**
  - **стандартного платежного приложения на карте МИР с выбором профиля по типу терминала (например, чтобы всегда отклонять транзакцию в случае провала ODA)**
  - **отдельного пополняемого кошелька**
- **Реализуется в различных форм-факторах (карта, часы, стикеры)**

Мобильное приложение «Мир»

Основные характеристики мобильного приложения «Мир»

- Реализуется в облачном ЭБ на мобильном устройстве с поддержкой Android 4.4.2+ (HCE)
- Реализуется в SDK, интегрируемом в мобильные приложения банков
- Поддерживает бесконтактные и удаленные платежи
- Все мобильные операции токенизируются в зависимости от домена использования токена (бесконтактные операции, удаленные платежи, Card-On-File, отдельные ТСП и т.п.) и мобильного устройства клиента
- Все операции обслуживаются в онлайновом режиме с обязательной верификацией держателя карты по ПИН-коду на мобильном устройстве
- Использование fingerprinting устройства (для аутентификации мобильного устройства и реализации защищенной БД на устройстве)
- Технологически полностью соответствует контактному + бесконтактному приложению «Мир» (наследуется формат объектов данных и команд)

Жизненный цикл карты «Мир»

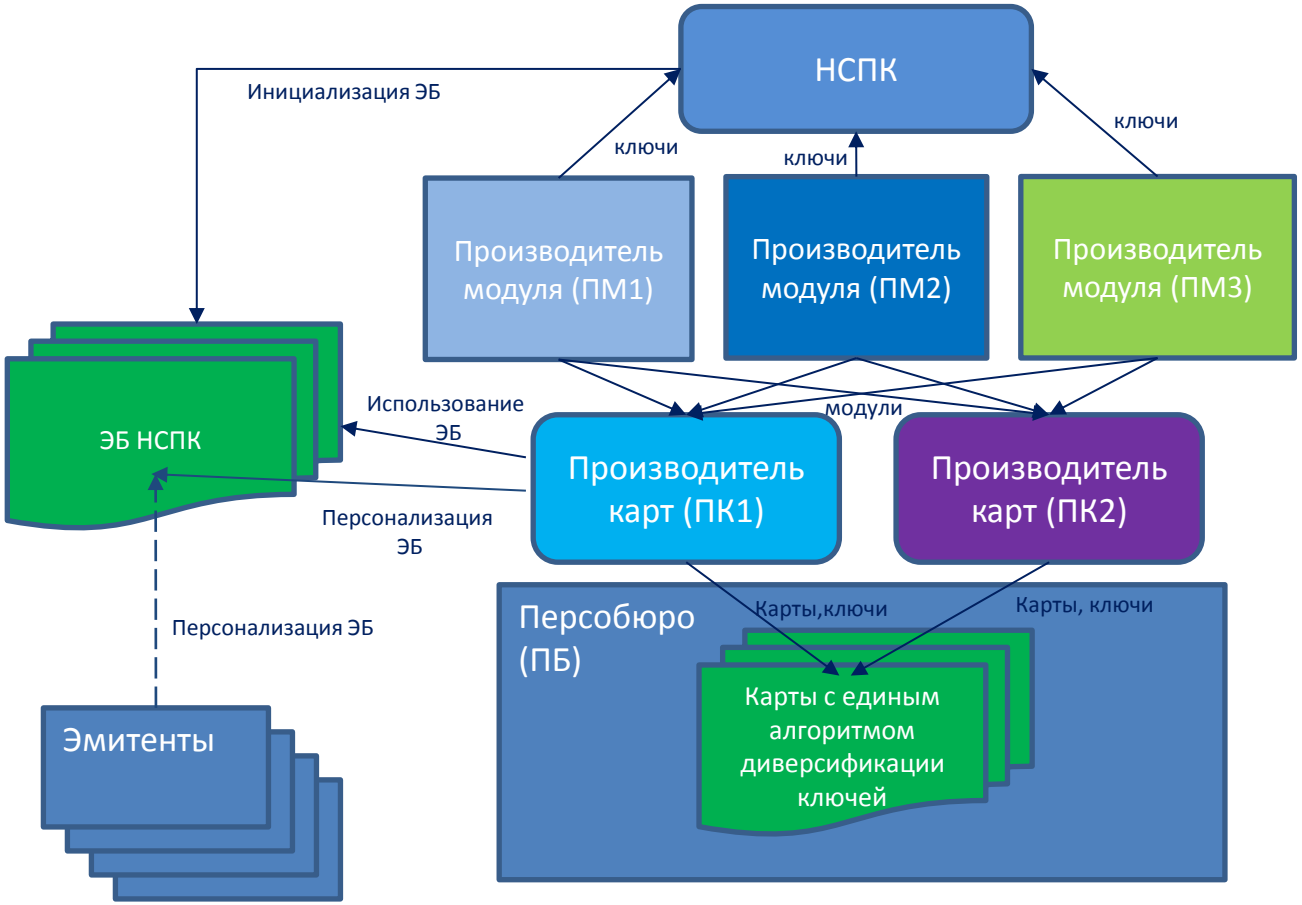
- Сертификация карты и инфраструктуры ее выпуска
- Подготовка карты
- Персонализация карты
- Использование карты для выполнения платежей

Сертификация карты «Мир» с точки зрения ее безопасности

Виды сертификации	Центр сертификации	Результат
Сертификация производителей модулей	НСПК	Реестр сертифицированных производителей модулей
Сертификация производителей карт	НСПК	Реестр сертифицированных производителей карт
Сертификация персобюро	НСПК	Реестр сертифицированных персобюро
Сертификация карты на безопасность	НСПК (проверка сертификатов EMVCo PCN или CC EAL 5+) Методика сертификации карты на безопасность	Реестр сертифицированных карточных платформ
Сертификация приложения по функциональности	НСПК	НСПК, в будущем аккредитованные лаборатории
Сертификация персонализации карты	НСПК	Проверка корректности персонализации приложения и разрешение банку эмитировать карты Мир

Выбор карточной платформы

- Банк может использовать карточную платформу из списка сертифицированных платформ, указанных на портале НСПК
- Если платформа несертифицирована, то она должна пройти сертификацию:
  - Если платформа открытая и используется cap-файл НСПК, то к ней предъявляются следующие требования до начала сертификации:
    - Java Card не ниже 2.2 (включая Java Card API, Java Card Runtime Environment и Java Card Virtual Machine, стандартные криптографические библиотеки и криптографический API);
    - GlobalPlatform версии 2.1.1 и выше;
    - наличие сертификатов:
      - ✓ EMVCo ICCN (Integrated Circuit Certificate Number);
      - ✓ EMVCo PCN (Platform Certificate Number) или Common Criteria (ISO 15408) по уровню не ниже EAL5+
  - Если платформа нативная, то в аккредитованной НСПК лаборатории выполняется сертификация платформы на безопасность в соответствии с Методикой оценки безопасности карты «Мир»



КМС-ПМ – мастер ключ, который НСПК предоставляет производителю модулей (ПМ). Данный ключ используется элементом безопасности (ЭБ) для загрузки приложения и ключей у производителя карт (ПК). В конце процедуры загрузки данный ключ меняется на КМС-ДБЭ

КМС-ППЭ – мастер ключ, на котором персо-бюро будет производить персонализацию приложения. Загружается в ЭБ ПК/Эмитентом. ЭБ выводит из него ключи и пре-персонализирует ими каждую карту после загрузки приложения

КМС-ДБЭ – мастер ключ домена безопасности эмитента

Персонализация карты «Мир»

- **Полное соответствие де-факто индустриальному стандарту EMV CPS 1.1**
- **Управление ключами полностью соответствует требованиям стандарта EMV CPS 1.1: K_{DEC}, K_{MAC}, K_{ENC}**
- **Объект KEYDATA для вывода ключей персонализации карты формируется и загружается в приложение на этапе подготовки карты (предперсонализации) и предоставляется машине персонализации в ответ на команду Initialize Update**
- **Для взаимной аутентификации карты и машины персонализации, обеспечения целостности и конфиденциальности данных, циркулирующих между картой и машиной персонализации, применяются сессионные ключи**

Особенности платежного приложения «Мир»

- Полное соответствие стандарту EMV 4.3. Стандартные механизмы безопасности EMV:
  - **Сессионная схема использования ключей**
  - **Взаимная аутентификация приложения и эмитента**
  - **Офлайновая динамическая аутентификация приложения (IDN)**
  - **Скрипт-процессинг (MAC, шифрование секретных данных)**
  - **Шифрование счетчиков в IAD при передаче эмитенту**
  - **Офлайн ПИН (проверка факта успешной верификации PIN Offline), Global PIN**
- Дополнительные механизмы безопасности:
  - **Счетчики/лимиты использования ключей**
  - Аутентификация терминала
  - Интернет ПИН
  - Защищенный обмен сообщениями с терминалом
  - CV-сертификаты с различными полномочиями терминалов
  - Контроль полномочий терминалов

Non-EMV функциональность платежного приложения «Мир»

- Взаимная аутентификация приложения и терминала
- ЗОС с терминалом (в том числе с внешним сервером)
- Интернет ПИН (дополнительный офлайновый ПИН для работы через недоверенную среду)
- Возможность работы с виртуальным терминалом (Интернет-хостом)
- Защищенное хранилище данных

Взаимная аутентификация карты с терминалом

Карта «МИР»

Виртуальный терминал

Проверка и извлечение открытого ключа **терминала**

Передача сертификатов сервис-провайдера и терминала

Проверка и извлечение открытого ключа **карты**

Передача сертификатов эмитента и карты

Используются секретный ключ **терминала** и открытый ключ **карты**

Обмен подписями и секретами

Используются секретный ключ **карты** и открытый ключ **терминала**

Вычисление сессионных ключей ЗОС на основе обоих секретов

Защищенный обмен сообщениями

- Устанавливается между приложением карты и (виртуальным) терминалом
- Всегда устанавливается после процедуры взаимной аутентификации терминала
- Используется уникальный счетчик команд в рамках текущей сессии (невозможно поменять порядок следования команд)
- Входные и выходные данные всех команд шифруются и подписываются
- Позволяет обмениваться чувствительными данными через открытые каналы (Интернет)

Интернет ПИН-код

- Хранится в приложении «Мир»
- Используется вместо ПИН-кода при выполнении операций в недоверенной среде, защищая ПИН от перехвата
- Может предъявляться напрямую, например, через специальные ридеры с ПИН-падом или через виртуальный терминал
- Вводится клиентом после проверки фразы контрольного приветствия

Защищенное хранилище данных

- Реализовано на базе стандартных EMV-записей
- Позволяет настраивать условия доступа индивидуально для каждой записи (в рамках SFI)
- Возможность добавлять новые SFI и записи в процессе жизненного цикла карты
- Возможность определить условия доступа к записям на этапе персонализации
- Возможность изменять условия доступа к записям в процессе жизненного цикла карты
- Возможность комбинировать различные условия доступа
- Предоставляет широкие возможности по реализации нефинансовых приложений

Разделение прав доступа к защищенному хранилищу данных

Режимы доступа

- Администрирование (изменение условий доступа)
- Чтение данных
- Обновление данных

Условия доступа (конъюнктивно-дизъюнктивная форма)

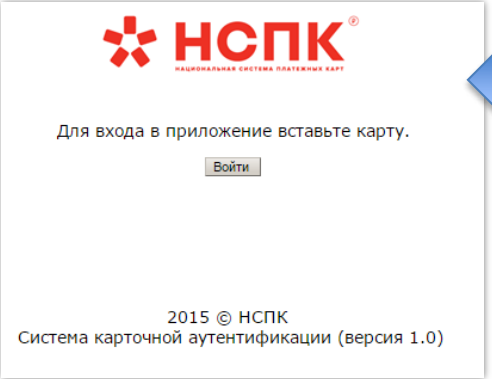
- Всегда
- Никогда
- Успешная проверка Офлайн ПИН
- Успешная проверка Интернет ПИН
- Взаимная аутентификация с терминалом и полномочиями указанными в CV-сертификате
- Механизм скрипт-процессинга

Пример: Аутентификация в ДБО

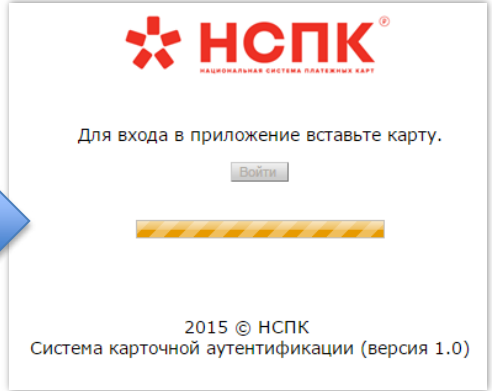
ПК со считывателем карт

- Клиент подключает к ПК считыватель карт
- Клиент заходит на сайт системы ДБО

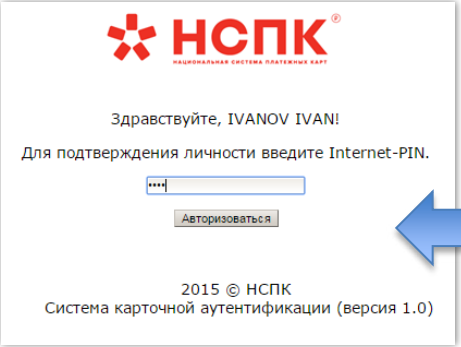
Система ДБО



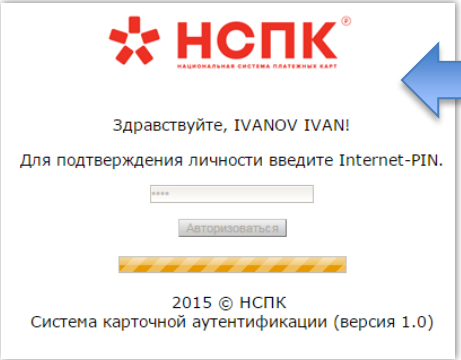
- Клиент вставляет карту «Мир» в считыватель карт
- Между картой «Мир» и системой ДБО устанавливается защищенное соединение



Пример: Аутентификация в ДБО



- По защищенному каналу:
  - Из защищенной области карты* считывается фраза контрольного приветствия и отображается клиенту
  - Проверив фразу, клиент предъявляет Интернет ПИН



- ДБО проводит EMV-AAC транзакцию с нулевой суммой

- В случае успешной проверки криптограммы система авторизует клиента

* Дополнительно может быть считан номер телефона для отправки SMS-кода подтверждения клиенту

Проведение транзакции в ДБО

ПК со считывателем карт

- Клиент подключает к ПК считыватель карт
- Клиент авторизуется в системе ДБО
- Клиент инициирует проведение транзакции
- Система подготавливает транзакционные данные
- Клиент вставляет карту МИР в считыватель карт
- Между картой и системой ДБО устанавливается защищенное соединение
- По защищенному каналу:
  - Из защищенной области карты считывается фраза контрольного приветствия и отображается клиенту
  - Проверив фразу, клиент предъявляет Интернет ПИН
  - ДБО проводит транзакцию и выполняет проверку криптограммы
  - В случае успешной проверки криптограммы система авторизует транзакцию

Система ДБО

НСПК

Спасибо
за внимание!

Российская
платежная система