НСПК

Безопасность карты «Мир»

Российская
платежная система

МИР

Голдовский Игорь Михайлович
Главный архитектор
АО «НСПК»

Содержание

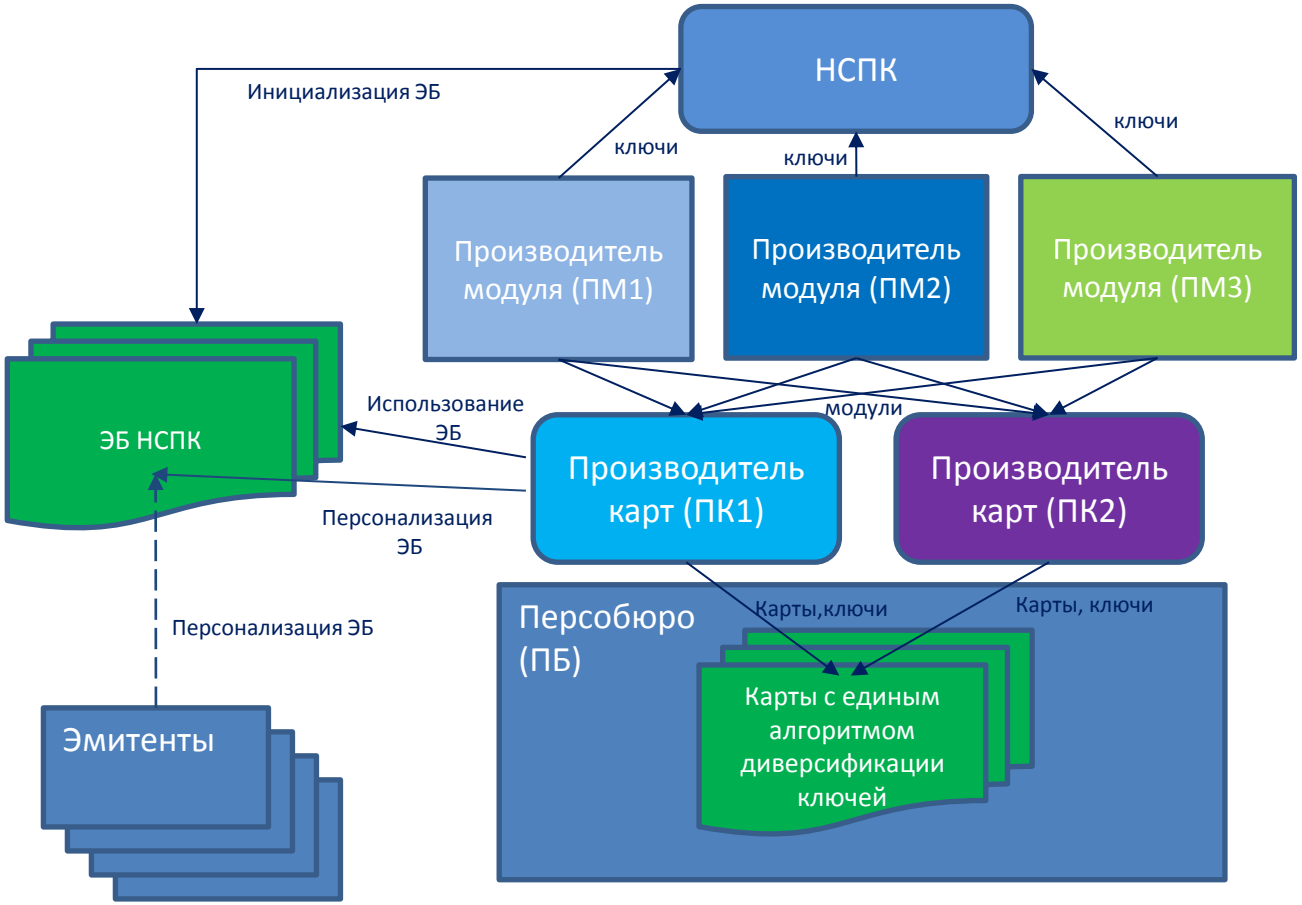
- Жизненный цикл карты «МИР»
- Требования к безопасности карты и карточной платформы
- Подготовка карты
- Персонализация карты
- Механизмы безопасности при выполнении операции
- Дополнительная функциональность приложения Мир: non-EMV функциональность

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, CC EAL 5+)	Реестр сертифицированных карточных платформ
Сертификация приложения (функциональное тестирование)	НСПК	НСПК, аккредитованные лаборатории
Сертификация персонализации карты	НСПК	Разрешение банку эмитировать карты Мир



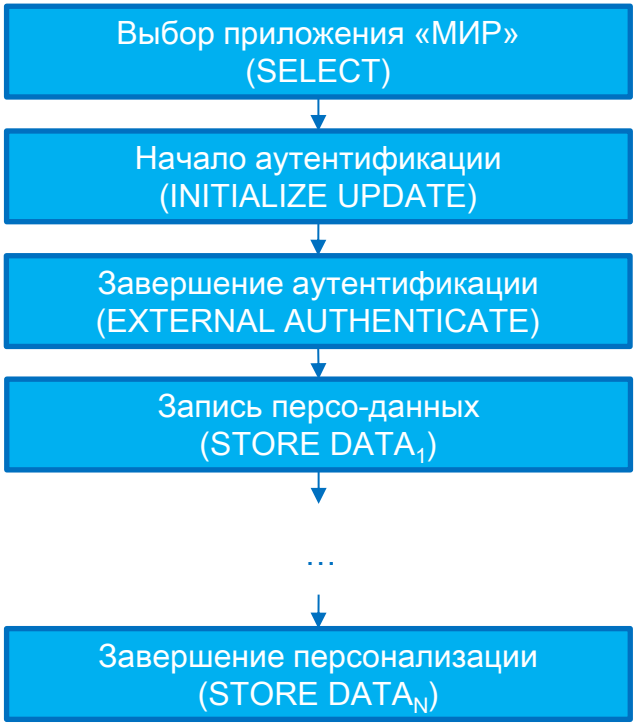
КМС-ПМ – мастер ключ, который НСПК предоставляет производителю модулей (ПМ). Данный ключ используется элементом безопасности (ЭБ) для загрузки приложения и ключей у производителя карт (ПК). В конце процедуры загрузки данный ключ меняется на КМС-ДБЭ

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

Производитель карт получает от производителя чипов модули и производит загрузку и установку приложения «МИР» После установки приложения производится его выбор, аутентификация на ключах домена безопасности и загрузка ключей для персонализации, KEYDATA

Персонализация карты Мир (CPS 1.1)



Процедура персонализации не зависит от производителя карты/чипа.

Используются единые алгоритмы диверсификации для всех карт

Ключи эмитента для персонализации приложения «Мир»

- Управление ключами полностью соответствует требованиям стандарта EMV CPS 1.1: K_{DEC}, K_{MAC}, K_{ENC}
- KEYDATA формируется и загружается в приложение на этапе подготовки карты (предперсонализации) и предоставляется машине персонализации в ответ на команду Initialize Update
- Для взаимной аутентификации карты, шифрования данных и обеспечения их целостности применяются сессионные ключи (полное соответствие стандарту EMV CPS 1.1)

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**
  - **Скрипт-процессинг**
  - **Шифрование счетчиков в IAD при передаче эмитенту**
  - **Офлайн ПИН, Global PIN**
- Дополнительные механизмы безопасности:
  - **Счетчики использования ключей**
  - Аутентификация терминала
  - Интернет ПИН
  - Защищенный обмен сообщениями с терминалом
  - CV-сертификаты, различные полномочия терминалов
  - Контроль полномочий терминалов

Защищаемые объекты данных приложения MPA

- **Primary Assets**:

- Симметричные мастер-ключи приложения (MK_{AC},MK_{SMI}, MK_{SMC}, MK_{IDN})
- Симметричные сессионные ключи приложения (SK_{AC},SK_{SMI}, SK_{SMC})
- Секретные ключи RSA: $S_{ICC-PIN}$ и S_{ICC-DA}
- Reference PIN Offline и Интернет-ПИН
- Публичные ключи RSA: $P_{ICC-PIN}$, P_{ICC-DA} и $P_{TERM-CA}$
- Ключи ЗОС для шифрования и обеспечения целостности

Защищаемые объекты данных приложения MPA

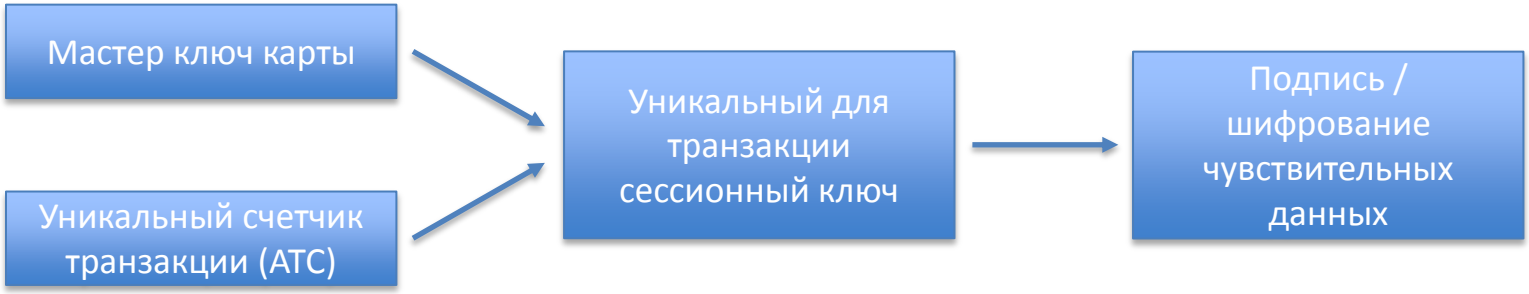
- **Secondary Assets**:

- ATC
- PTC
- PIN Decipherment Counter/PIN Decipherment Counter limit
- SK SMI counter/SK SMI limit
- SK AC counter/SK AC Limit
- Verify Terminal Certificates Counter/Verify Terminal Certificates Limit

Другие защищаемые объекты

- Исходный код приложения: мошенники могут получить доступ к ключам и другим секретам приложения и даже клонировать карту
- Состояния автомата состояний приложения
- Случайные числа, генерируемые приложением

Сессионная схема использования ключей



- Дополнительная защита мастер ключа карты
- В случае компрометации сессионного ключа после выполнения транзакции его дальнейшее использование злоумышленником невозможно
- Используется в процессе
  - генерации криптограммы
  - обработки скриптовых команд
  - установки защищенного обмена сообщениями с терминалом

Ключи приложения 1/2

Ключ	Назначение
Мастер ключ карты для вычисления криптограммы (MK_{AC})	Создание сессионного ключа (SK_{AC}), который используется при генерации криптограммы приложения
Мастер ключ карты для обеспечения целостности скриптовых команд (MK_{SMI})	Создание сессионного ключа (SK_{SMI}), который используется для проверки подписи скриптовых команд
Мастер ключ карты для обеспечения конфиденциальности скриптовых команд (MK_{SMC})	Создание сессионного ключа (SK_{SMC}), который используется для расшифровки данных скриптовых команд
Мастер ключ карты для вычисления IDN (MK_{IDN})	Создание динамического кода приложения (ICC Dynamic Number) для валидации эмитентом

Ключи приложения 2/2

Ключ	Назначение
Секретный ключ приложения (S_{ICC})	Используются в процедурах аутентификации приложения (также может быть использован для расшифрования ПИН и аутентификации терминала)
Секретный ключ для шифрования ПИН ($S_{ICC-PIN}$)	Используется для расшифрования полученного от терминала ПИН-кода
Секретный ключ для шифрования секрета карты ($S_{ICC-TERM-AUTH}$)	Используется для шифрования секрета карты при организации ЗОС

Лимиты использования ключей

Ключ	Используется	Назначение
SK_{AC}	При обработке ответа от хоста эмитента (ARPC)	Защита от подбора значения ключа карты (MK_{AC}) путем перебора ARPC
SK_{SMI}	При обработке скриптовых команд	Защита от подбора значения ключа карты (MK_{SMI}) путем перебора MAC-кода скриптовых команд
$S_{ICC-PIN}$ / S_{ICC}	При проверке PIN Offline	Защита от подбора значения ключа карты ($S_{ICC-PIN}$ / S_{ICC})
$S_{TERM-CA}$ $S_{TERM-ISS}$	При аутентификации терминала	Защита от попыток подбора ключей $S_{TERM-CA}$ и $S_{TERM-ISS}$

Офлайновая аутентификация данных приложения

Динамическая аутентификация данных (DDA):

- На секретном ключе карты шифруются следующие данные:
  - Случайное число, полученное от терминала
  - ICC Dynamic Number
- Защита целостности данных карты
- Невозможность создания копии карты

Комбинированная аутентификация данных (CDA):

- На секретном ключе карты шифруются следующие данные:
  - Случайное число, полученное от терминала
  - ICC Dynamic Number
  - Тип криптограммы карты (CID)
  - Криптограмма карты
  - Хэш-функция данных, передаваемых в командах GPO, Generate AC и ответе на первую команду Generate AC
- Защита целостности данных карты
- Невозможность создания копии карты
- Защита от wedge-атак

Схема взаимодействия УЦ и Банка (EMV)

Банк эмитент СЭДО НСПК

Формат запроса на сертификат ключа банка

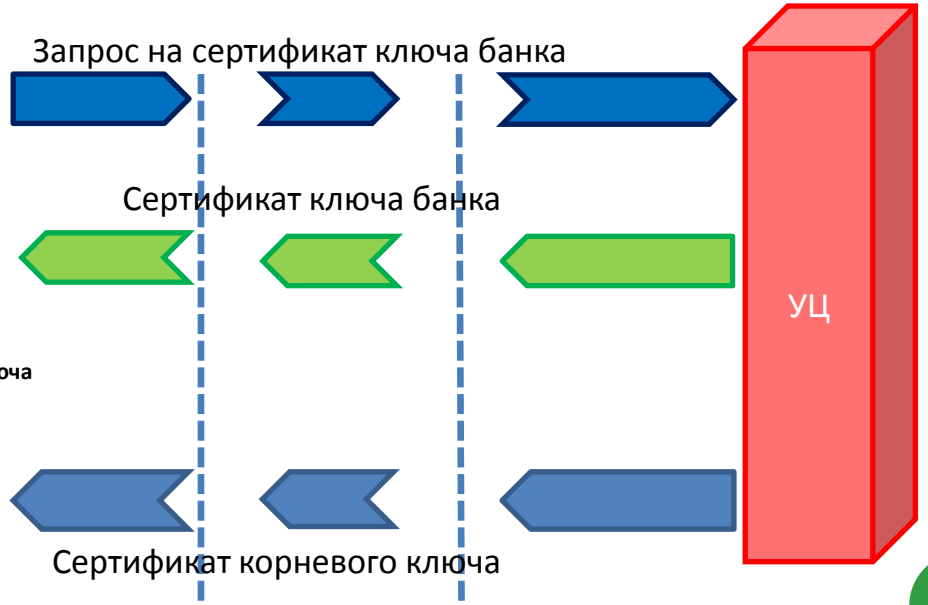
- Открытая часть ключа банка
- Номер запроса
- Срок действия сертификата
- Идентификатор сервиса (PIX)
- Идентификатор эмитента (IIN)
- Контрольная сумма
- Подпись ключа банка

Формат Сертификата ключа банка

- Идентификатор сервиса (PIX)
- Идентификатор эмитента (IIN)
- Серийный номер сертификата
- Срок действия сертификата
- Номер корневого ключа
- Контрольная сумма
- Подпись на корневом ключе

Формат Сертификата корневого ключа

- Номер корневого ключа
- Открытая часть корневого ключа
- Код приложения провайдера (RID)
- Срок действия ключа
- Контрольная сумма
- Подпись ключа



Банк эквайер

PIN Offline

- Хранится на карте «Мир»
- Предъявляется POS-терминалом локально
- Как правило, шифруется при передаче на карту
- Разгружает систему эмитента / ОПКЦ и ускоряет выполнение операции
- Лимит числа попыток ввода ПИН-кода определяется эмитентом карты и может принимать значения от 1 до 15 (обычно равен 3)

Механизм проверки факта проверки картой PIN Offline

Стандартная обработка PIN Offline подвержена атаке: wedge-устройство может подменить ответ/эмулировать ответ карты на команду Verify (проверка PIN Offline)

Для защиты используется специальный механизм:

- При генерации криптограммы терминал передает карте результат проверки PIN Offline
- Карта «Мир» параллельно отслеживает статус проверки PIN Offline
- В случае, если терминал заявляет, что ПИН успешно проверен, а на карте стоит статус – ПИН не проверялся или проверялся не успешно, то карта отклоняет транзакцию или отправляет ее на авторизацию эмитенту с указанием в CVR бита “PIN Offline wrongly considered OK”

Изменение данных приложения (скриптовые команды)

- **Отправляются на карту в процессе или после выполнения транзакции**
- **Подписываются на ключах эмитента**

Назначение:

- **Изменение значений лимитов**
- **Изменение настроек системы управления рисками**
- **Разблокировка ПИН-кодов**
- **Разблокировка приложения**
- **Изменение пользовательских данных**

Non-EMV функциональность платежного приложения «Мир»

- Возможность работы с виртуальным терминалом (Интернет-хостом)
- Поддержка CV-сертификатов
- Взаимная аутентификация с терминалом
- ЗОС с терминалом (в том числе с виртуальным)
- Интернет ПИН (дополнительный офлайновый ПИН для ЭК)
- Разграничение прав доступа в зависимости от терминала для доступа к данным
- Возможность проведения операций по бесконтактному интерфейсу
- Требует сохранения на карту небольшого объема дополнительных данных на этапе персонализации

CV-сертификаты

- **CV (Card Verifiable) – сертификат, проверяемый картой**
- **два вида сертификатов: терминала и сервис-провайдера**
- **содержат список полномочий**
- **полномочия терминального сертификата не могут быть выше полномочий сертификата сервис-провайдера**
- **подпись предоставляется отдельно от сертификата**

Взаимная аутентификация карты с терминалом

Карта «МИР»

Виртуальный терминал

Передача сертификатов сервис-провайдера и терминала

Проверка и извлечение открытого ключа **терминала**

Передача сертификатов эмитента и карты

Проверка и извлечение открытого ключа **карты**

Обмен подписями и секретами

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

Вычисление сессионных ключей ЗОС на основе обоих секретов

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

Защищенный обмен сообщениями

- **Устанавливается между картой 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 на карте «Мир»
- Используется вместо офлайн ПИН-кода при выполнении
- Может предъявляться хостом (виртуальным терминалом)
- Может предъявляться напрямую, например, через специальные ридеры с Пин-падом
- Защищает офлайн ПИН-код от перехвата
- Должен вводиться клиентом после проверки фразы контрольного приветствия

Пример полномочий сертификатов

Описание полномочия	Полномочия сервис-провайдера	Полномочия терминала 1 (Интернет)	Полномочия терминала 2 (Стандартный)
Можно читать внутренние объекты приложения (BFxx)	**Нет**	**Нет**	**Нет**
Можно читать данные приложения (записи SFI 01-0A)	Да	Да	Да
Можно выполнять Script Processing	Да	Да	Да
Можно выполнять Generate AC	Да	Да	Да
Можно проводить верификацию Интернет-ПИН	Да	Да	**Нет**
Можно проводить верификацию Офлайн-ПИН	Да	**Нет**	Да
Можно работать по бесконтактному интерфейсу	Да	Да	**Нет**
Можно работать по контактному интерфейсу	Да	Да	Да
Можно создавать записи приложения (Create Record)	Да	Да	Нет

Полномочия терминала (определены в CV-сертификате)

- Полномочия по использованию лишь определенных профилей приложения
- Полномочия по манипулированию записями в SFI, отличных от файлов EMV, имеют формат arwxxxxx, где:

➢ a (бит 8)- флаг доступа на администрирование

➢ r (бит 7)- флаг доступа на чтение

➢ W (бит 6)- флаг доступа на изменение записи SFI

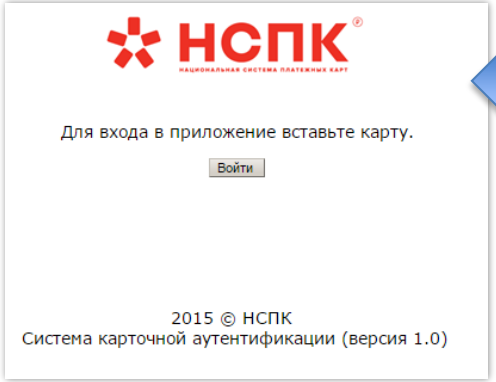
➢ xxxxx- SFI файла

Пример: Аутентификация в ДБО

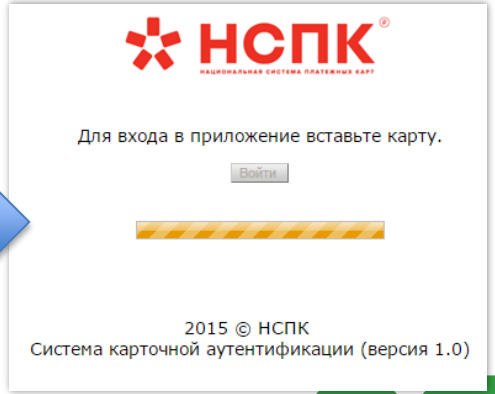
ПК со считывателем карт

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

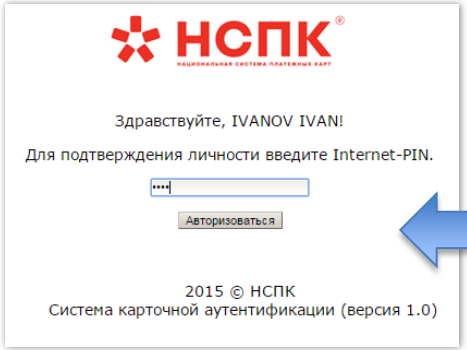
Система ДБО



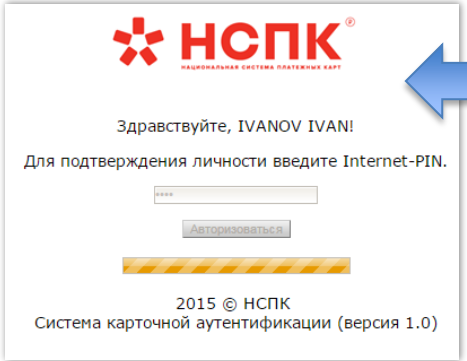
- Клиент вставляет карту «Мир» в считыватель карт
- Между картой «Мир» и системой ДБО устанавливается защищенное соединение



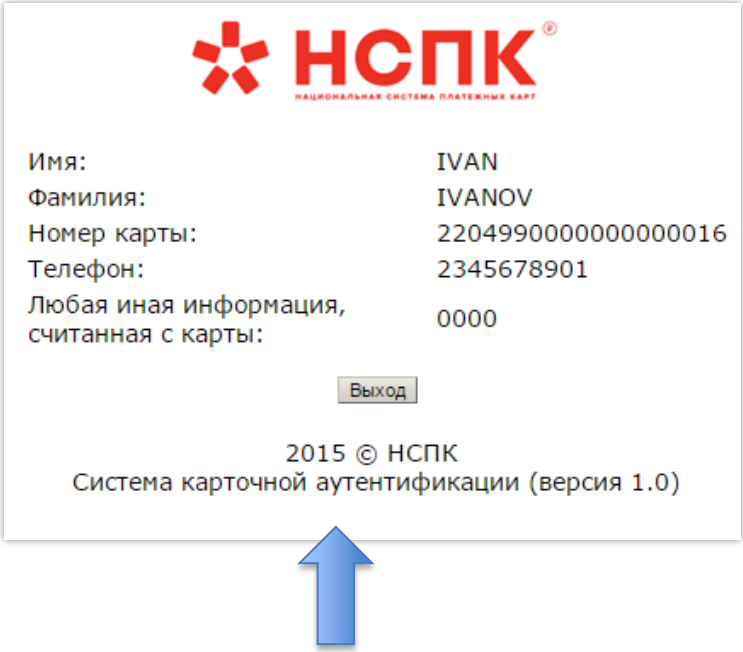
Пример: Аутентификация в ДБО



- 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 данные для подписи транзакции (TDS)
- Клиент вставляет карту «Мир» в считыватель карт
- Между картой «Мир» 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 EMV-AAC транзакцию с нулевой суммой (включая контрольную сумму TDS-данных в функцию вычисления криптограммы)
  - В случае успешной проверки криптограммы система авторизует транзакцию

Система ДБО

НСПК

Спасибо
за внимание!

Российская
платежная система