MirAccept 2.0

Основы для технических специалистов ПСП и Иностранных Участников

Порядок тестирования и подключения

Ковачев Виталий
Главный технический администратор Платформы 3-D Secure
Операционно-технологический Департамент АО «НСПК»

Структура презентации

Блок 1:

1. Что такое MirAccept и зачем он нужен
2. Возможности MirAccept 2.0: каналы, категории сообщений
3. Иерархия версий 3DS
4. Схемы подключения ПСП (Эмитент, Эквайрер)
5. Схемы подключения Участников ПС МИР (Эмитент, Эквайрер)

Блок 2:

1. Предварительная подготовка
2. Создание задачи на подключение
3. Проведение испытаний 3DS
4. NIV тестирование
5. Подготовка к выходу в ПРОД (ETED, MAF, CRF)
6. Выход в ПРОД

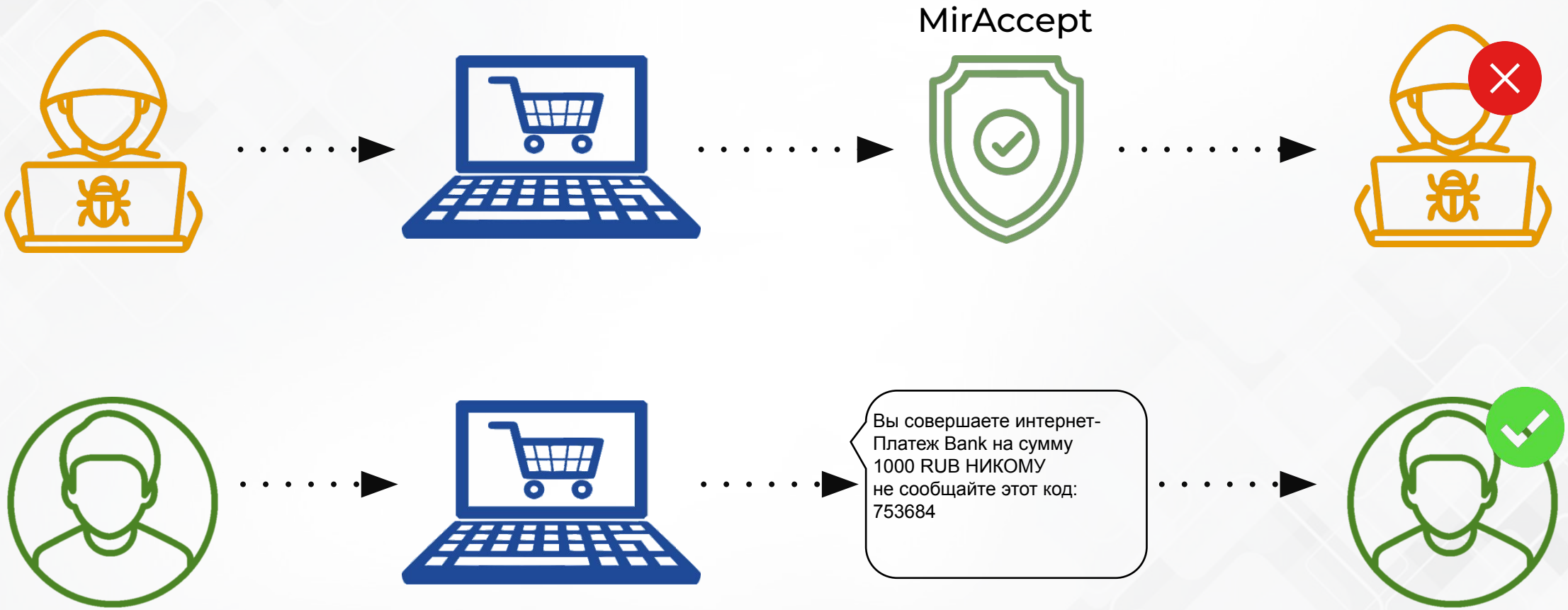
Блок 3:

1. Новое в EMV 3DS 2.2.0

Блок 1

Что такое MirAccept и зачем он нужен?

Что такое MirAccept и зачем он нужен



Что такое MirAccept и зачем он нужен

MirAccept – это протокол надежной аутентификации Держателей карт, основанный на EMV 3DS 2.0, позволяющий:

1. Подтверждать принадлежность используемого при проведении операции платежного средства его владельцу
2. Препятствовать проведению мошеннических операций
3. Повышать доверие Держателей карт к электронной торговле.
4. Не терять конверсию и при этом повысить удобство держателя карты, сохраняя высокий уровень безопасности
5. При успешной аутентификации - перенос ответственности на Эмитента в случае возникновения диспута

Версии MirAccept

MirAccept 1.0 – устаревший протокол надежной аутентификации, Эмитентами ПС «Мир» более не используется.

Полная миграция Эквайреров с него планируется до конца 2022 года

MirAccept 2.0 – современный протокол надежной аутентификации, активно используется в ПС «Мир».
Поддерживает два варианта реализации:

- EMV 3DS 2.1.0 - обязательный
- EMV 3DS 2.2.0 - опциональный

Возможности MirAccept 2.0

EMV 3DS:

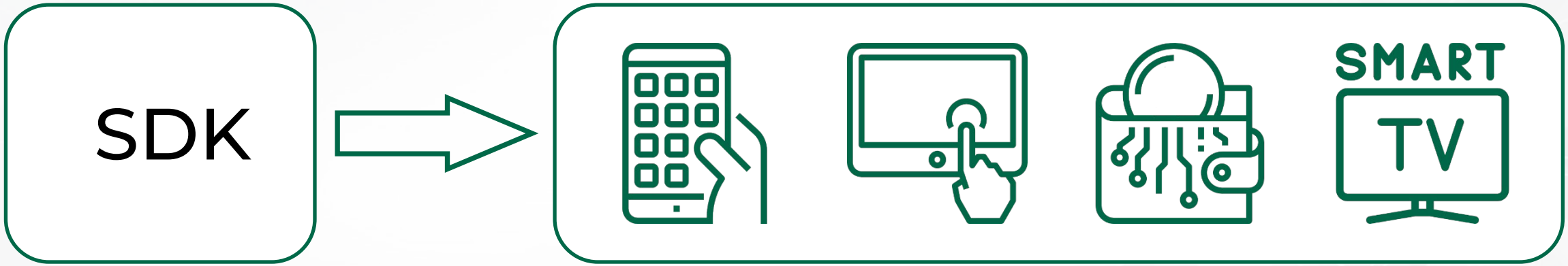
- Каналы инициирования (BRW,APP,3RI)
- Категории сообщений (PA|NPA)
- Сценарии аутентификации
- Версии спецификаций

MirAccept 2.0 - Поддержка браузеров

Привычный канал совершения платежей в Интернет.
Для оценки риска помимо расширенного набора данных используется Browser Fingerprint

MirAccept 2.0 - Поддержка мобильных устройств

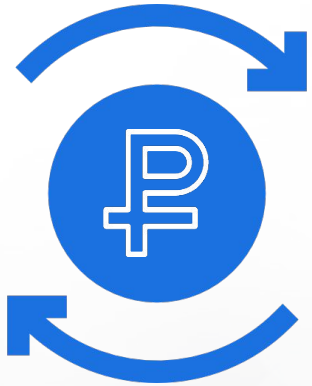
Аутентификация держателя карты может быть выполнена при совершении операций с любых носимых устройств при помощи встраиваемого SDK (Application-based 3DS)



MirAccept 2.0 - Поддержка 3RI

3RI (3DS Requestor-Initiated) – аутентификация ТСП держателя карты, инициированная без участия держателя

Основной сценарий использования – выполнение повторяющихся/регулярных платежей
(оплата по подпискам на сервисы, оплата по счетам и т.д.)



Категория сообщений

Платежная аутентификация
Message Category
01-PA

Покупка/оплата

Device Channel

Приложение – 01-APP

Браузер – 02-BRW

Инициировано в ТСП – 03-3RI (только 2.2.0)

Неплатежная аутентификация
Message Category
02-NPA

Проверка/привязка карты

Device Channel

Приложение – 01-APP

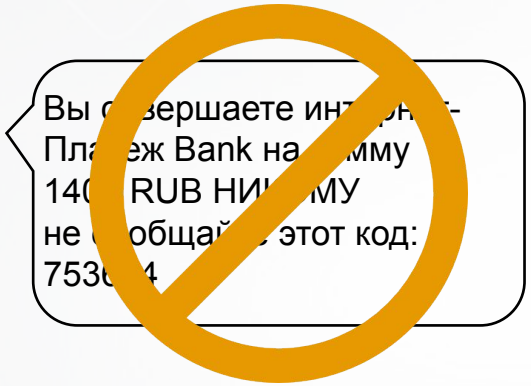
Браузер – 02-BRW

Инициировано в ТСП – 03-3RI

MirAccept 2.0 – Frictionless Flow

3D Secure аутентификация держателя без взаимодействия с ним:

- не требует дополнительных действий от клиента
- повышает конверсию для ТСП
- обеспечивает высокий уровень безопасности



MirAccept 2.0 – СПР

Главное преимущество: избавляет Эмитента от необходимости устанавливать и обслуживать собственную систему рискового анализа

MirAccept 2.0 – анализ рисков

Решение по Frictionless/Challenge аутентификации принимает Эмитент на основе анализа рисков в режиме реального времени

Расчет рисков выполняется

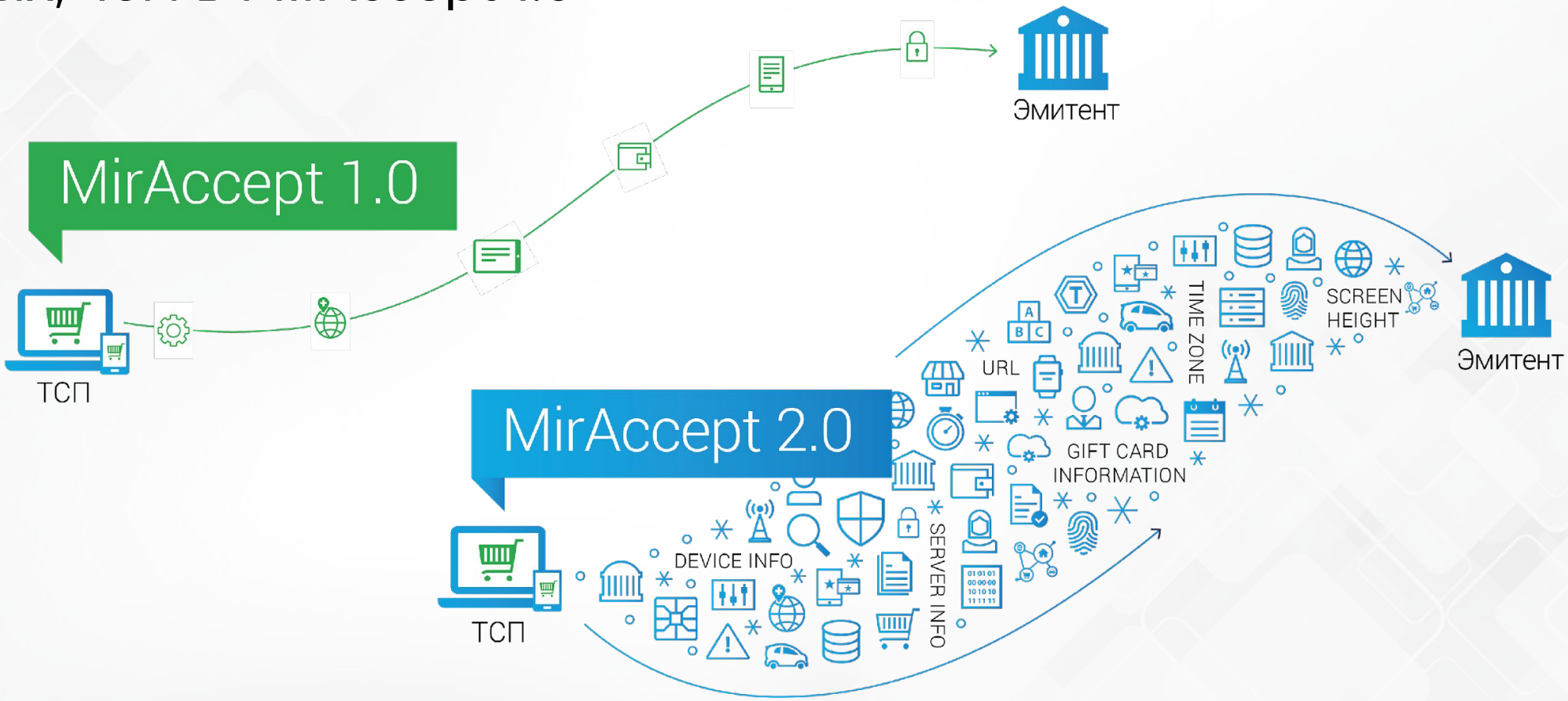
Эмитентом (самостоятельно)

и/или

Сервисом Принятия Решений (СПР)

MirAccept 2.0 – анализ рисков

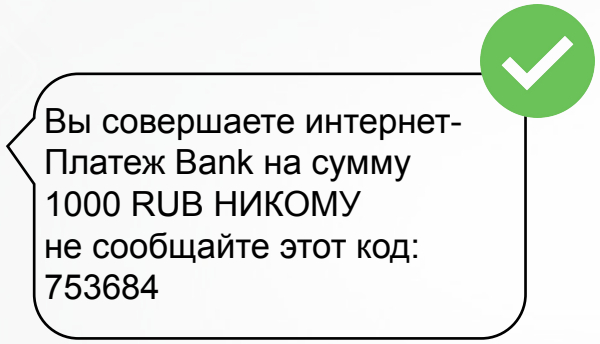
Для принятия взвешенного решения необходим анализ большого количества данных. Используется примерно в 10 раз больше данных, чем в MirAccept 1.0

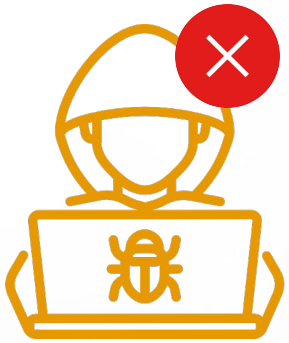


MirAccept 2.0 – Challenge Flow

3D Secure аутентификация по результату взаимодействия с держателем:

- «Классический» сценарий 3D Secure
- обеспечивает безопасность в ситуации, когда высок риск мошеннической операции





Сервис Attempt ПС «Мир»

Сервис Attempt – обязательный сервис для всех Участников, предоставляемый в рамках сервиса MirAccept.

Основная задача сервиса – перенос финансовой ответственности на эмитента при проведении операций аутентификации, когда ACS эмитента не может обеспечить сервис на своей стороне.

Сервис предоставляется в обязательном порядке для всех карт ПС «Мир» и тарифицируется в соответствии с Правилами ПС «Мир»

Сценарии Attempt ПС «Мир»

С технической точки зрения Attempt – это сценарий операции, вызванный невозможностью ACS Эмитента аутентифицировать держателя

Невозможность осуществить аутентификацию может быть вызвана следующими причинами:

- Сетевая не доступность серверов ACS Эмитента
- Превышено время ожидания ответа от ACS Эмитента
- Держатель карты не участвует в сервисе MirAccept
- Держатель карты не зарегистрирован на MirAccept на ACS Эмитента либо не может быть аутентифицирован

Сервис Attempt формирует собственную криптограмму NSPK-CAV в соответствии с форматом и на криптографических ключах ПС «Мир».

Валидация авторизации с помощью проверки “NSPK-MAC”

Основная задача - предотвращение фальсификации Эквайером реквизитов авторизации, а также для того, чтобы установить ответственного в случае мошеннической операции.

Особенности работы проверки NSPK-MAC

- Фронт система НСПК вычисляет NSPK-MAC на основании реквизитов авторизации и проверяет соответствие полученного в авторизационном запросе NSPK-MAC рассчитанному значению.
- Значения в авторизационном сообщении должны полностью совпадать со значениями элементов данных, отправленными и полученными в ходе аутентификации
- Если проверка не пройдена, то операция передается Эмитенту, как Non-3DS, то есть с переносом ответственности на Эквайрера

Иерархия версий EMV 3DS

Версия	Дата публикации	Статус	Комментарий
2.0.1	Март 2017	Устарела	Первая «черновая» версия спецификации
2.1.0	Октябрь 2017	Активна	Первая «релизная» версия спецификации
2.2.0	Декабрь 2018	Активна	Вторая версия спецификации
2.3.0	Сентябрь 2021	Опубликована	Третья версия спецификации

Сертификация НСПК DS версии 2.2.0

Компания НСПК 21 мая 2021 года успешно завершила сертификацию собственного продукта DS по последней версии спецификации EMV 3DS 2.2.0

Approval / Reference Number: 3DS_LOA_DIS_NPCS_020200_00409

Активные версии EMV 3DS в MirAccept 2.0

EMV 3DS 2.1.0 – базовый протокол,
поддерживает следующие возможности:

- Сценарии: Frictionless & Challenge
- Каналы: BRW, APP, 3RI (только неплатежная)
- Категории: платежная, неплатежная

EMV 3DS 2.2.0 – следующая версия протокола,
в дополнение к 2.1.0 поддерживает:

- Платежную аутентификацию в 3RI
- Отложенную аутентификацию (Decoupled)
- Белые списки (whitelisting)

MirAccept 2.0

Схемы подключения Участников и ПСП:

- в роли Эмитента
- в роли Эквайрера

Схема подключения Эквайрера ПС МИР

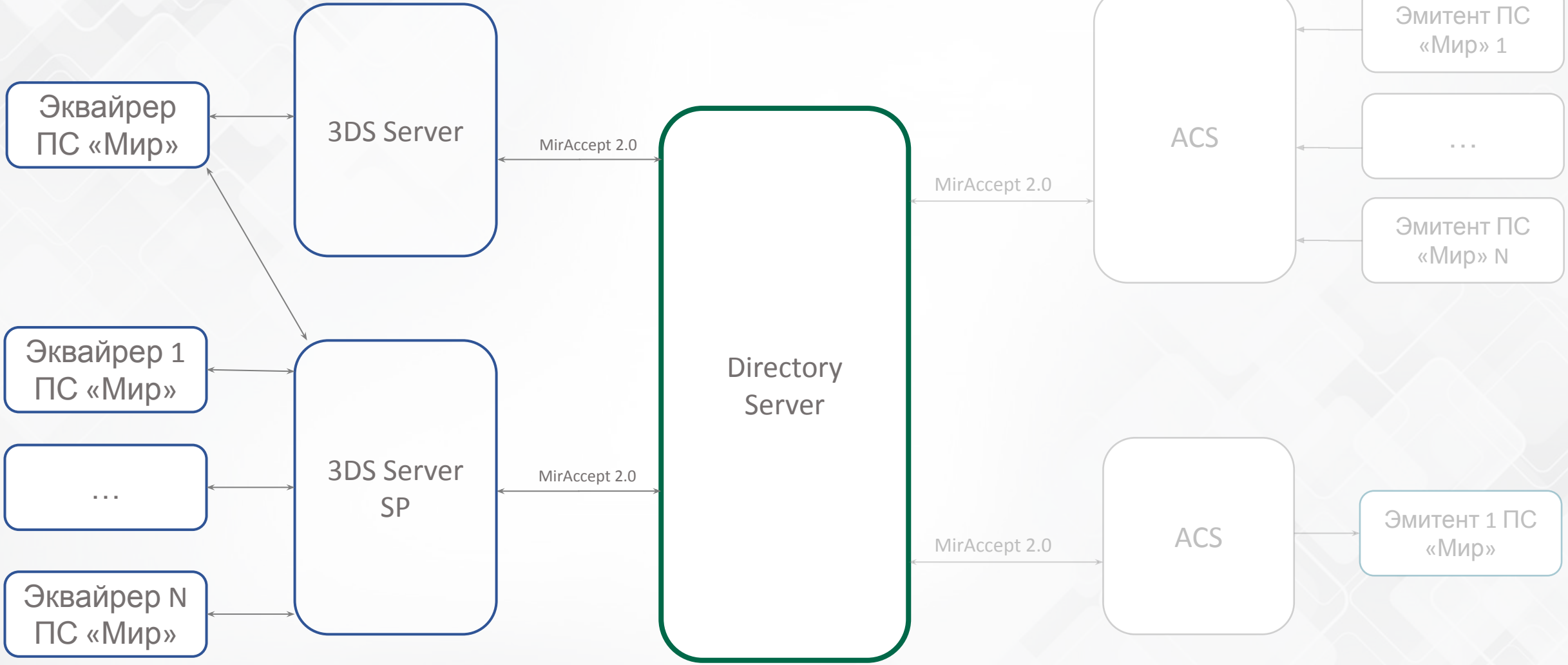


Схема подключения Эквайрера ПСП

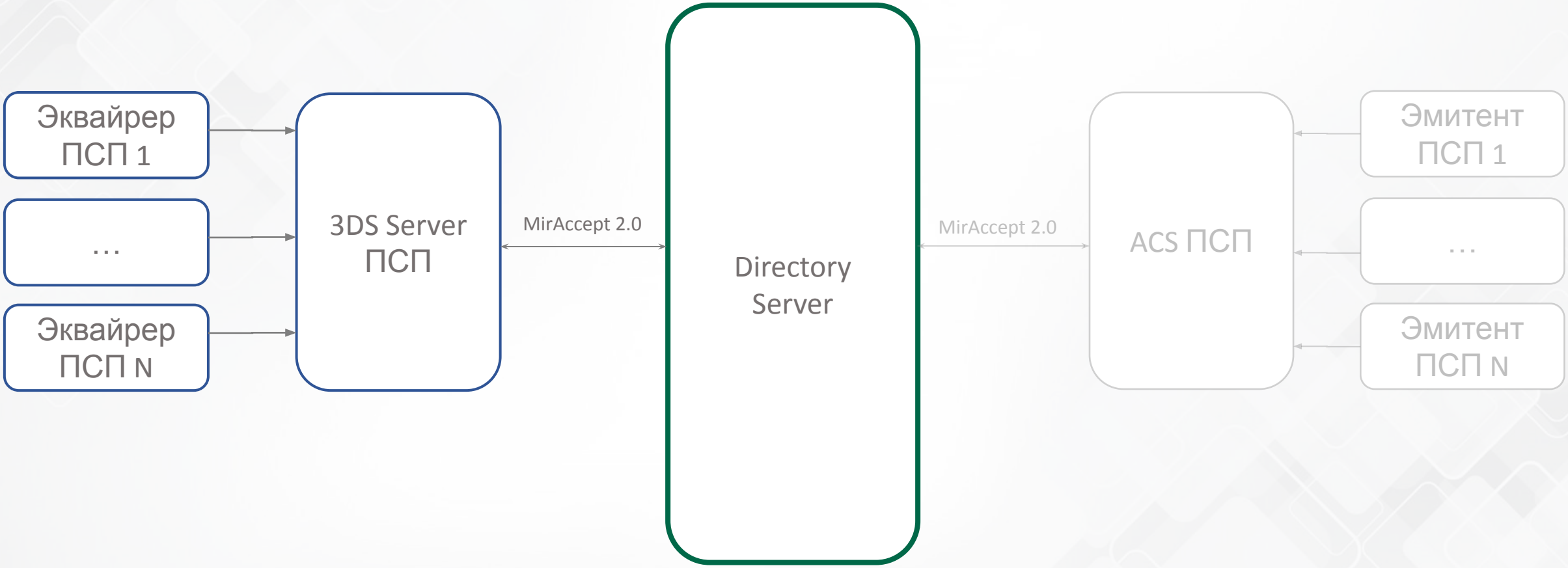


Схема подключения Эмитента ПС МИР

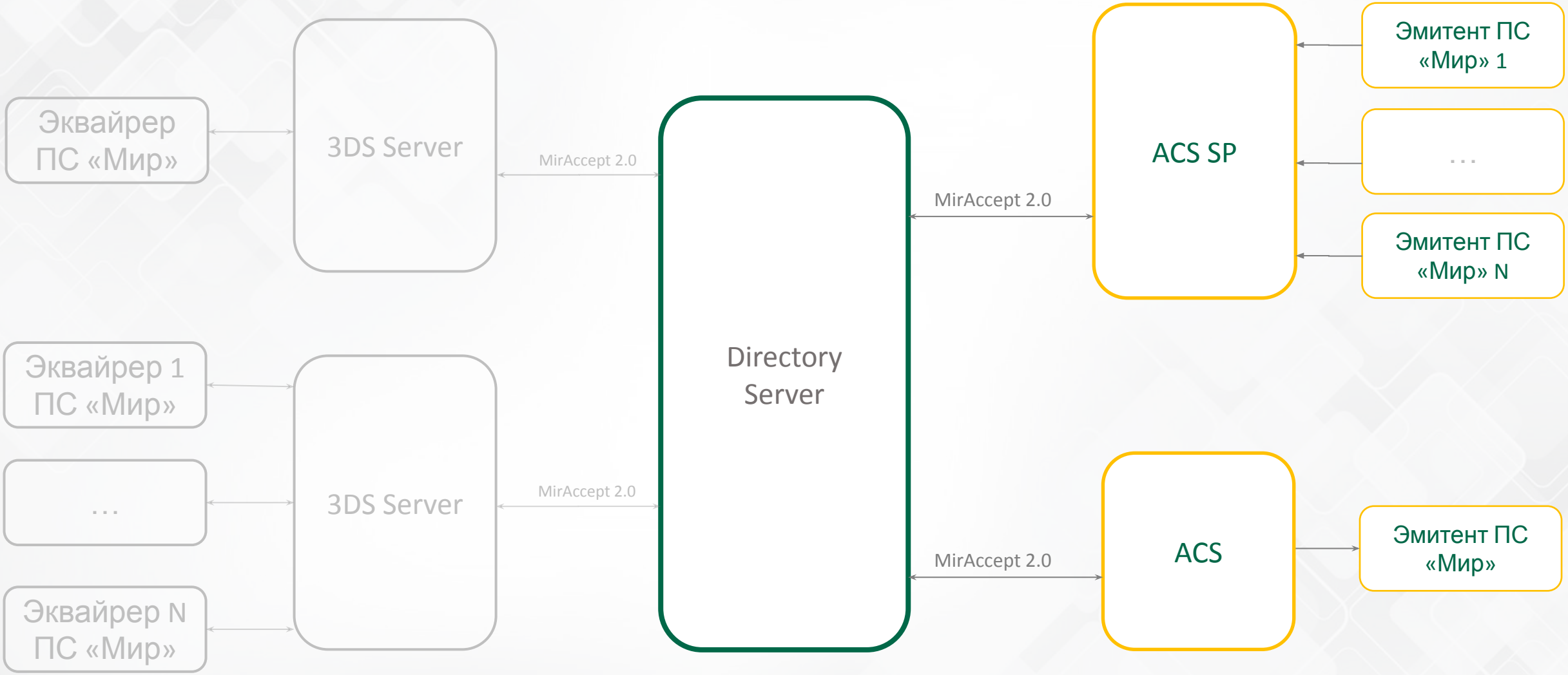


Схема подключения Эмитента ПСП

Блок 2

1. Предварительная подготовка
2. Создание задачи на подключение
3. Проведение испытаний 3ds
4. NIV тестирование
5. Подготовка к выходу в ПРОД (ETED, MAF, CRF)
6. Выход в ПРОД

Общий “timeline” процесса подключения

1. Предварительная подготовка
2. Создание задачи на подключение
3. Проведение испытаний 3ds
4. NIV тестирование
5. Подготовка к выходу в ПРОД (ETED, MAF, CRF)
6. Выход в ПРОД

Предварительная подготовка

1

Предварительная подготовка

- Определиться с вендорским решением
- Приступить к подготовке тестовой и ПРОД инфраструктуры
- Получить доступ на портал НСПК
- Изучить документацию по проведению тестирования

Реестр одобренных Вендоров

- Содержит актуальный перечень Вендорских решений (ACS или 3DSServer), прошедших аутентификационное тестирование в НСПК
- Содержит информацию о поддерживаемых типах аутентификации: Browser-Based, Application-Based, 3RI
- Содержит актуальные Reference Number для использования в Продакшн Среде

Для российских Участников

Для ПСП и иностранных Партнеров

Общая документация для Эквайеров (для Участников и ПСП)

Основополагающим документом для Эквайеров для выполнения процесса по выходу в ПРОД является : Стандарт ПС Мир. MirAccept 2.0. Руководство по внедрению для Эквайрера_v.1.7.pdf

Документация содержит:

- Описания требований , предъявляемых ПС МИР к компоненту 3DSServer для того чтобы осуществить его настройку, параметризацию, понять детали и особенности интеграции с DS НСПК
- Порядок действий и требуемые шаги для выхода в ПРОД
- Примеры заполнения файлов MAF
- Требования к аутентификаций/авторизаций
- Требования к сертификатам и криптографическим величинам

Общая документация для Эмитентов (для Участников и ПСП)

Основополагающим документом для Эмитентов для выполнения процесса по выходу в ПРОД является : Стандарт ПС Мир. MirAccept 2.0. Руководство по внедрению для Эмитента_v.1.7.pdf

Документация содержит:

- Описания требований , предъявляемых ПС МИР к компоненту ACS для того чтобы осуществить его настройку, параметризацию, понять детали и особенности интеграции с DS НСПК
- Порядок действий и требуемые шаги для выхода в ПРОД
- Примеры заполнения файлов CRF
- Требования к обработке аутентификаций/авторизаций
- Требования к сертификатам и криптографическим величинам

Основная документация для проведения тестирования (для Участников и ПСП)

Стандарт платежной системы «Мир». Сервис MirAccept. Руководство по проведению тестовых испытаний подключения к сервису для Участников и Вендоров — RU

Mir PS Standard. MirAccept Service Connection Testing Guidelines for Participants and Vendors — EN

Указанные документы доступны в соответствующих разделах Портала НСПК для Участников и ПСП

Depicted documents are available in the related sections on NSPK Support Portal for Participants and PSP

Документация для тестирования 3DSServer (для Участников и ПСП)

- Приложение 6. Заявка-Акт тестовых испытаний аутентификационного взаимодействия при подключении MirAccept (Участник) 2.1.0 и 2.2.0.xlsx
- Приложение 4. Аутентификационные тест-кейсы для тестирования 3DS Server 2.1.0.xlsx
- Приложение 9. Аутентификационные тест-кейсы для тестирования 3DS Server 2.2.0.xlsx

Documentation for (Participants and PSP) 3DSServer tests

- Appendix 6. Certificate-Request for Authentication Interaction Testing when connected via MirAccept 2.1.0 and 2.2.0 (Participant).xlsx
- Appendix 4. Authentication Test Cases for 3DS Server 2.1.0 Testing.xlsx
- Appendix 9. Authentication Test Cases for 3DS Server 2.2.0 Testing.xlsx
- Mir PS Standard. MirAccept Service Connection Testing Guidelines for Participants and Vendors_v.1.2.pdf

Документация для тестирования ACS (для Участников и ПСП)

- Приложение 6. Заявка-Акт тестовых испытаний аутентификационного взаимодействия при подключении MirAccept (Участник) 2.1.0 и 2.2.0.xlsx
- Приложение 3. Аутентификационные тест-кейсы для тестирования ACS 2.1.0.xlsx
- Приложение 8. Аутентификационные тест-кейсы для тестирования ACS 2.2.0.xlsx

Documentation for (Participants and PSP) ACS tests

- Appendix 6. Certificate-Request for Authentication Interaction Testing when connected via MirAccept 2.1.0 and 2.2.0 (Participant).xlsx
- Appendix 3. Authentication Test Cases for ACS 2.1.0 Testing.xlsx
- Appendix 8. Authentication Test Cases for ACS 2.2.0 Testing.xlsx
- Mir PS Standard. MirAccept Service Connection Testing Guidelines for Participants and Vendors_v.1.2.pdf

Создание задачи на подключение

Создание задачи в разделе “_Подключение”

В задаче необходимо указать:

- Тип подключаемого компонента 3DSServer/ACS
- версия/версии EMV 3DS
- наименование вендора ПО
- имя домена FQDN
- форма подключения (In-house либо площадка третьесторонней организации (IPSP));
- идентификатор Operator ID* (3DS или ACS);
- идентификатор Member ID;
- скриншоты платежных страниц/страниц интернет-магазинов, оформленные товарными знаками «Мир» и MirAccept в соответствии с требованиями документа

Выпуск сертификатов x509

Участник

Дождаться получения от НСПК значения Organizational Unit для использования его при выпуске сертификатов x509

НСПК

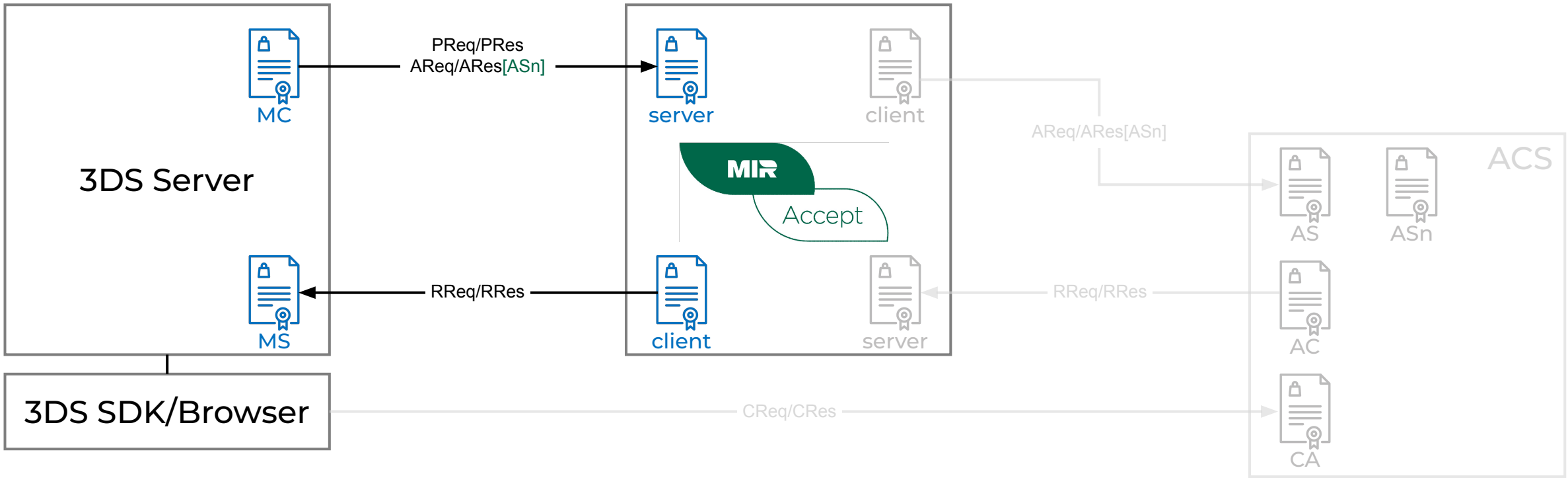
Открывает задачу для тестовых сертификатов x509 в разделе «07. Криптография (Наименование Участника)»

Участник

Прикрепляет к задаче на выпуск сертификатов сгенерированные запросы *.csr

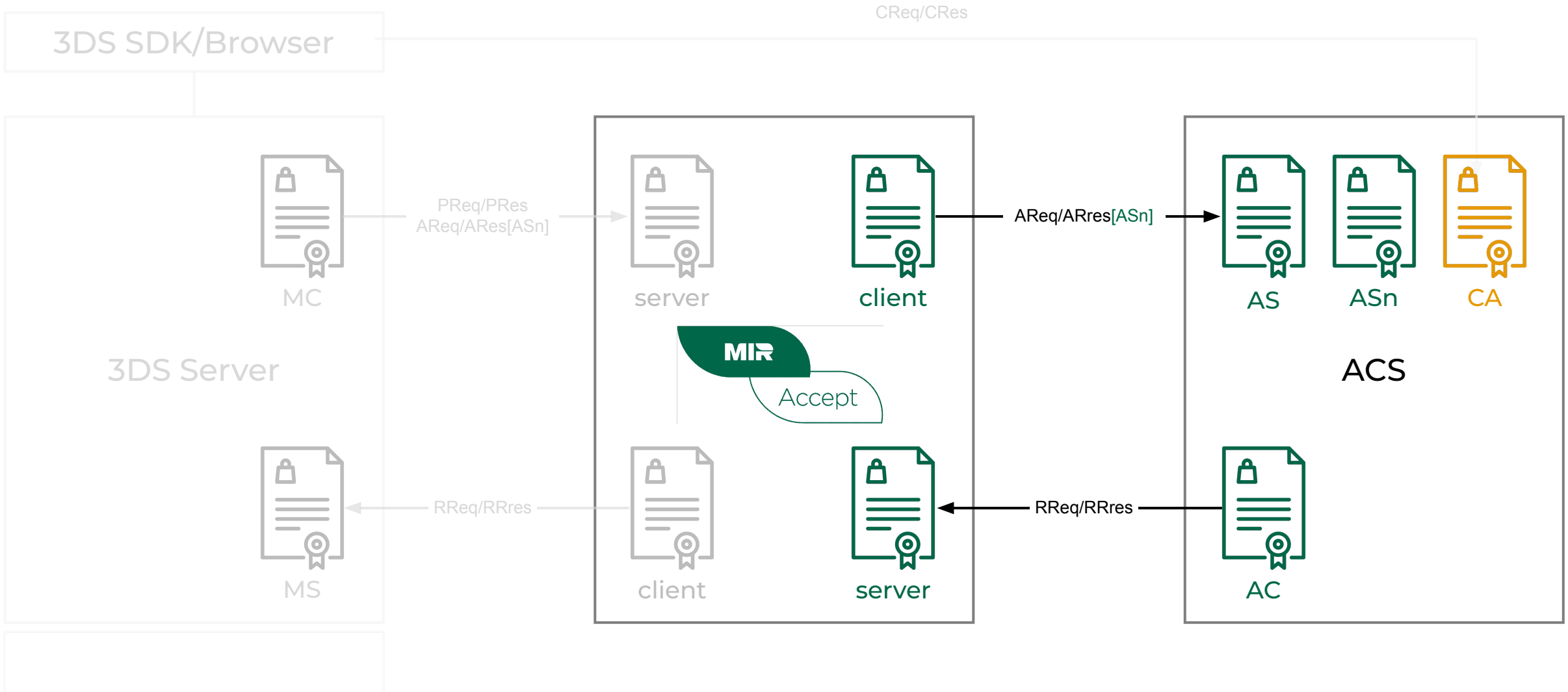
Распределение сертификатов. Эквайрер

* Все выпускаемые сертификаты для Эквайерера, подписываются промежуточным удостоверяющем центром MPISubCA в составе структуры PKI - корневого УЦ НСПК CA



Распределение сертификатов. Эмитент

* Все выпускаемые сертификаты для Эмитента, подписываются промежуточным удостоверяющем центром ACSSubCA в составе структуры PKI - корневого УЦ НСПК CA



Выпуск сертификатов X509

3DSServer

- Северный сертификат Server (MS)
- Клиентский сертификат Client (MC)

ACS

- Северный сертификат Server (AS)
- Клиентский сертификат Client (AC)
- Signing-сертификат (ASn)
- Сертификат стороннего УЦ (CA)

* Участнику, ранее уже выполнившему подключение MirAccept 2.0 по версии EMV 3DS 2.1.0, при подключении версии EMV 3DS 2.2.0 получение отдельных сертификатов не требуется

Настройка компонент для работы x509

3DSServer

- Настройка серверного сертификата x509 :
  MS (MPI Server) выданный УЦ НСПК
- Добавление в доверенное корневое хранилище сертификата **УЦ НСПК**
- Для Эквайреров с собственным SDK требуется **добавить корневой УЦ НСПК в компонент SDK**, для валидации acsSignedContent при проведении App-based

ACS

- Настройка серверного сертификата x509 :
  AS (ACS Server) выданный УЦ НСПК
- Настройка клиентского сертификата :
  AC (ACS Client) выданный УЦ НСПК
- Настройка сертификата подписи ASn для App-based сценария
- Настроен сертификат стороннего CA (для взаимодействия клиента с страницей аутентификации ACS)

Документация по безопасности

Основополагающим документом, регламентирующим процесс получения предоставления сертификатов RSA x509, описан в :

Регламент оказания услуг Удостоверяющего центра АО «НСПК» в рамках предоставления платежных сервисов

Настройка ACS

- Для настройки и тестирования с НСПК используются промышленные идентификаторы:
  - Organizational Unit (OU)
  - acsReferenceNumber (равный выданному Вендорскому LOA)
  - acsOperatorId (равный OU, выданного сертификата x509)
- Перед проведением тестирования Участник или ПСП передает в НСПК данные о диапазонах тестовых карт, ACS URL и 3DS Method URL (опционально)

Настройка 3DS Server

Для настройки и тестирования с НСПК используются промышленные идентификаторы:

- Organizational Unit (OU)
- threeDSRequestorID - (равный OU, выданного сертификата x509)
- threeDSServerOperatorID - (равный OU, выданного сертификата x509)
- threeDSServerRefNumber (равный выданному Вендорскому LOA)
- acquirerBIN – назначается НСПК для тестовых целей
- acquirerMerchantID – назначается НСПК для тестовых целей

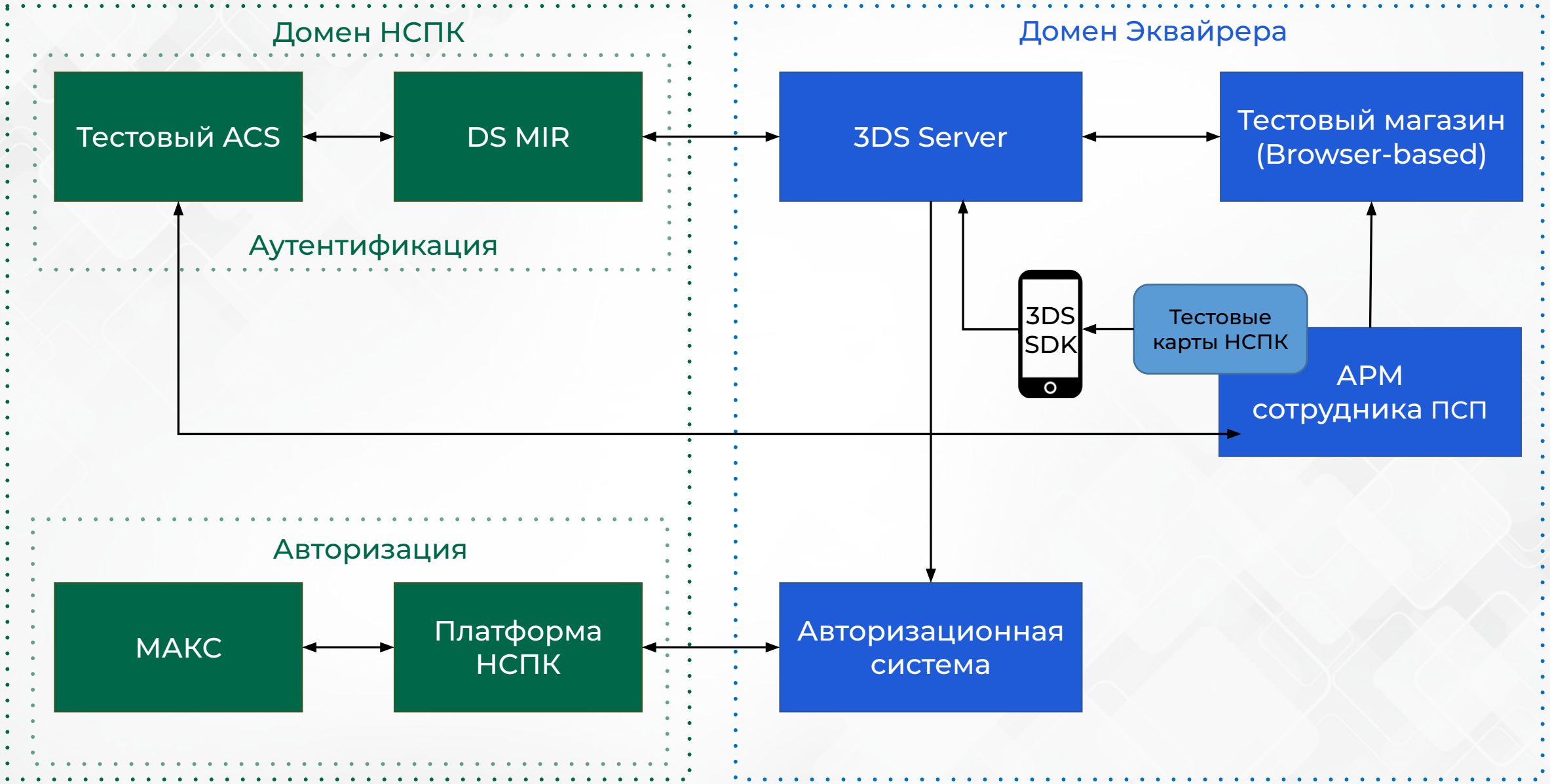
В задаче на тестирование получить от НСПК реквизиты тестовых сущностей, а также получить тестовое наименование ТСП для настройки на стороне 3DSServer

Резюмируем

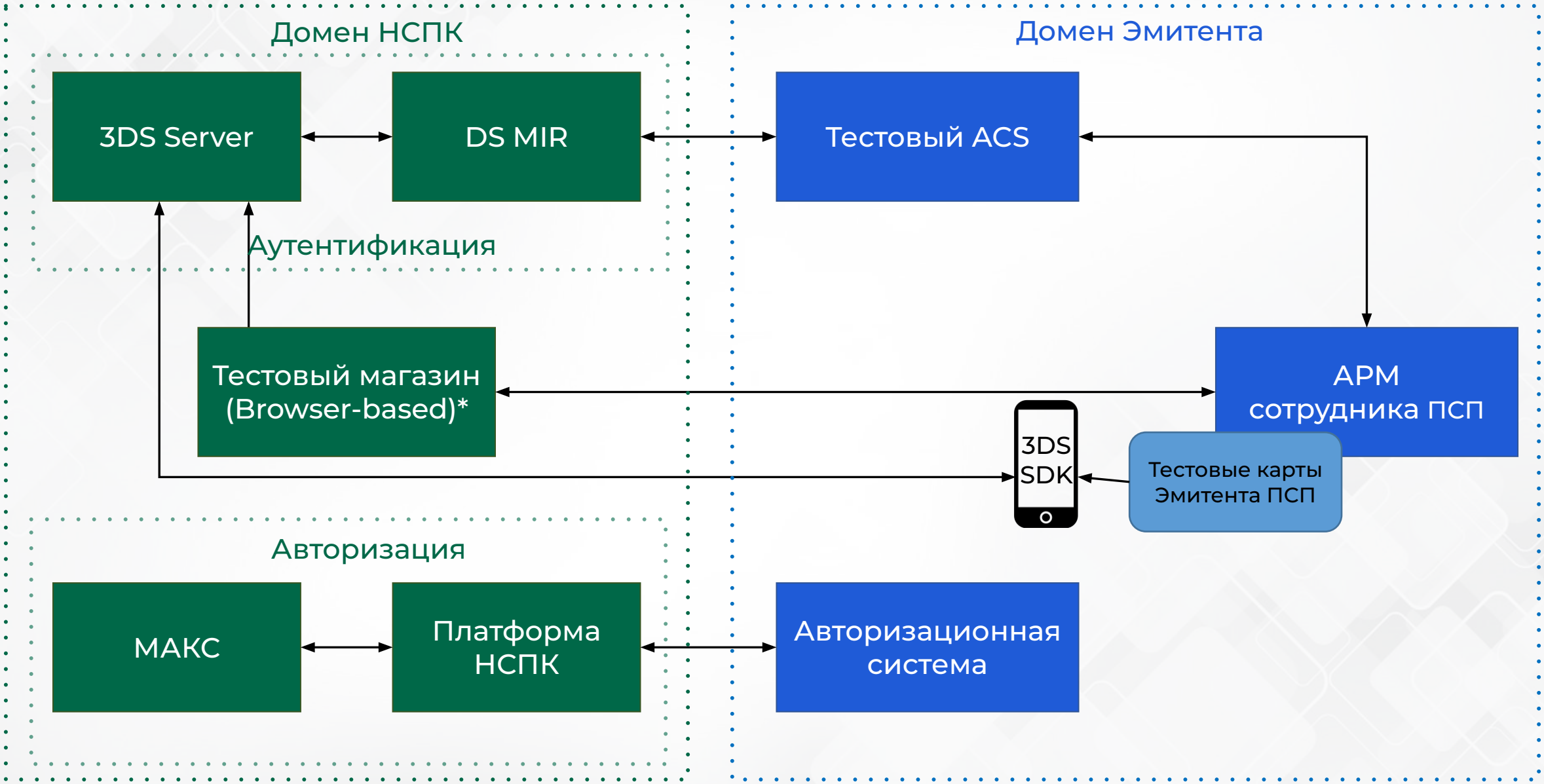
1. Заведена задача на Подключение, а также связанные задачи на выпуск тестовых и боевых комплектов сертификатов x509. Заведены необходимые задачи на аутентификационное тестирование Участника или ПСП
2. Произведена настройка в компонентах 3DSServer и ACS выпущенных сертификатов x509
3. На стороне тестовой и промышленной сред Участника или ПСП завершено открытие необходимых сетевых доступов МСЭ (меж сетевых экранов)
4. Для тестовой среды произведена настройка сущностей Эквайерера и Эмитента в компонентах 3DSServer и ACS
5. Для того, чтобы начать тестирование от Участника или ПСП не требуется отдельного подтверждения, можно приступить к проведению тестов по готовности.

Проведение испытаний 3DS

Среда для тестирования 3DS Server/SDK

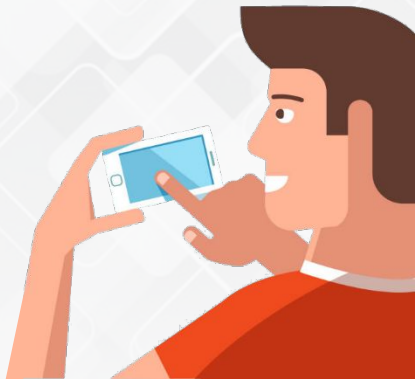


Среда для тестирования ACS



https://matool.vendorcert.mirconnect.ru/

Тестовое приложение НСПК с SDK для Android



Набор тест-кейсов 2.1.0 (Mandatory/Optional)

Для Вендоров

100%

тест-кейсов
обязательны

Для Участников и ПСП

~50%

тест-кейсов
обязательны

Набор тест-кейсов 2.2.0 (Mandatory/Optional)

Для Вендоров

100%

тест-кейсов
обязательны

Для Участников и ПСП

~50%

тест-кейсов
обязательны

Проведение тестирования 3DS Server/ACS в НСПК

В задаче на тестирование аутентификации:

Предоставляются ссылки на всю необходимую документацию

Предоставляется Test App/SDK (для тестирования ACS)

Сопровождается процесс тестовых испытаний

Осуществляется операционно-технологическая поддержка Вендора/Участника по любым вопросам, касающимся тестирования

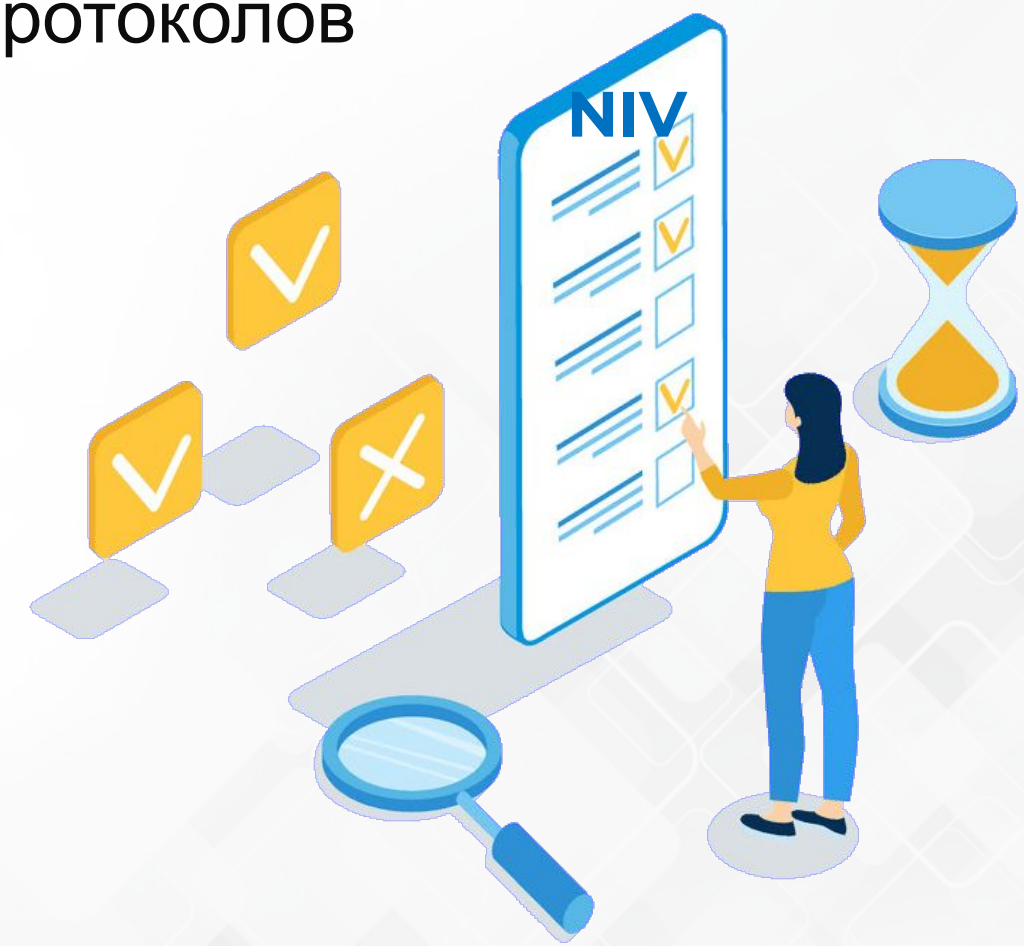
После финального проведения тест-кейсов:

- Список пройденных тест-кейсов с dsTransID прикладывается к задаче
- Тест-кейсы верифицируются НСПК
- НСПК выкладывает в задаче Акт проведения тестовых испытаний
- Оформленный Акт направляется Участником или ПСП в НСПК в двух экземплярах

4. NIV-тестирование в НСПК

NIV-тестирование в НСПК

NIV-тестирование – процесс подтверждения соответствия межхостового взаимодействия Участника или ПСП спецификациям протоколов ПВУ или NIPF



NIV-тестирование в НСПК (документация)

- Процедура проведения тестовых испытаний межхостового взаимодействия Участника ПС «Мир»
- Спецификация протокола ПВУ
- Руководство пользователя симулятора МАКС
- Стандарт Платежной системы Мир. Формирование и обработка Операций

и другие

Вся необходимая документация по порядку проведения NIV тестирования будет предоставлена Участнику или ПСП на портале НСПК, в рамках задачи по NIV тестированию

5. Подготовка к выходу в ПРОД (ETED, MAF, CRF)

1. Участник или ПСП получает промышленные сертификаты
2. Участник или ПСП по СЭДО направляет CRF/MAF файл С 1 ТСП или 1 range для ЕТЕД
3. Участник проводит успешный ЕТЕД
4. В задаче на Портале в разделе «_Подключение» согласуется дата вывода в промышленную эксплуатацию
5. Участник или ПСП по СЭДО направляет полный CRF/MAF файл
6. В назначенную дату НСПК подтверждает выполнение конфигурации Участника или ПСП в промышленной среде
7. Осуществляется пост-мониторинг промышленных операций

Обмен данными с НСПК - MAF

Основные поля MAF :

- AcquirerID – Эквайринговый бин, присвоенный в ПС МИР
- 3DSServerOperatorID – уникальный идентификатор endpoint 3DSServer равный значению OU выданного сертификата x509.
- MerchantID– Идентификатор точки обслуживания, в которой выполняется операция по карте
- MerchanName – наименование ТСП
- Action – действие, которое необходимо произвести с записью, возможные значения :
  - ADD – добавить
  - DEL – удалить
  - UPD – обновить
- RiskScoring– управление настройками Сервиса Принятия Решений, настраивается для каждого ТСП

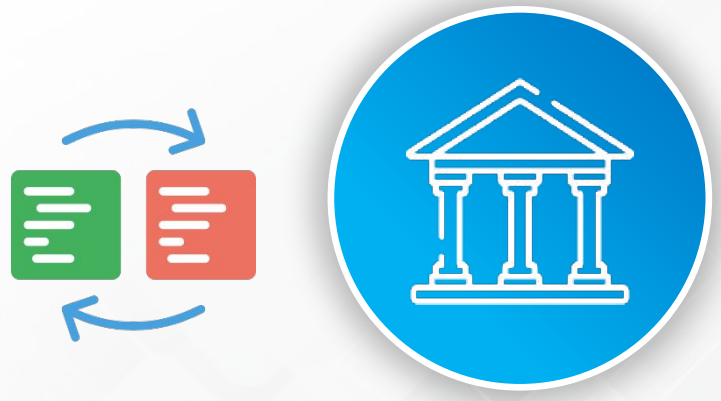
Обмен данными с НСПК - CRF

Основные поля CRF :

- BIN – 6 или 8-значный Эмиссионный бин, присвоенный в ПС МИР
- Begin Range – начало заданного карточного диапазона, подписанных на Miraccept 2.0
- End Range – конец заданного карточного диапазона, подписанного на Miraccept 2.0
- ACS1 URL – полный ACS URL для обслуживания аутентификаций в Miraccept 2.0. В данном параметре задается один URL, в CRF есть возможность также указать резервный ACS2 URL
- ACS1 Operator ID – уникальный идентификатор endpoint ACS равный значению OU выданного сертификата x509. В данном параметре задается один Operator ID, в CRF есть возможность также указать резервный ACS2 Operator ID
- ACS1 3DS METHOD URL - полный URL к собственному 3DS Method на стороне инфраструктуры ACS, в CRF также есть возможность указать дополнительный адрес резервного ACS2 3DS METHOD URL
- Route Through TRS – признак подписки диапазона на сервис СПР

Особенности параметризации в ПРОД для ПСП и Участников

Для ПСП MAF содержит информацию обо всех точках всех банков-Участников, находящихся “за ПСП” – это необходимо учитывать при формировании файла MAF



Для ПСП CRF - содержит все рейнжи всех банков Участников ПСП - ПСП должны агрегировать у себя все настройки всех Эмитентов “за ПСП” и формировать суммарный файл CRF.

5. Выход в ПРОД

Предварительная подготовка → Начало подключения → Проведение испытаний 3ds → NIV тестирование → Подготовка к выходу в ПРОД (ETED, MAF, CRF) → Выход в ПРОД

Выход в промышленную эксплуатацию выполнен!

ПРОД - среда 24\7 – качество сервиса наша общая цель

Профильные подразделения Участника должны регулярно:

1. Отслеживать новости на портале НСПК, связанные с обновлениями DS НСПК и другой важной информацией, влияющей на непрерывность предоставления сервиса

2. Отслеживать новости про публикуемые Технологические и операционные бюллетени НСПК –
   - анализировать изменения статей ТБ, связанные с сервисом MirAccept
   - своевременно планировать обновления на стороне своих компонент
   - своевременно проводить тестирование компонент на тестовой среде для поддержки изменений ТБ
   - Своевременно реагировать на задачи, создаваемые сотрудниками НСПК на портале поддержки

Контроль за сертификатами X509

1. Участники или ПСП должны самостоятельно отслеживать сроки действия выданных сертификатов x509 для компонент 3DSServer и ACS и производить своевременную замену (до даты истечения)

2. Выпуск обновленных сертификатов производится через заведение отдельной задачи на портале НСПК или создание заявки в системе КриптоМИР

Отслеживание изменений и настроек CRF и MAF

1

Требуется своевременно отправлять обновленный CRF в НСПК в случаях:

- Появления новых карточных диапазонов
- Изменение настроек MirAccept по существующим диапазонам, например смена ACS URL или ACS Operator ID
- Поддержка новой версии EMV 3DS
- Подключение СПР
- Любых других случаях, связанных с изменением подписки диапазонов Эмитента на сервис MirAccept

2

Требуется своевременно отправлять обновленный MAF в DS НСПК в случаях:

- Добавление, обновление и удаление ТСП
- Изменение Merchant Name, Merchant Url и других параметров имеющихся ТСП
- Изменение параметров подписки СПР или иное
- Любых других случаях, связанных с изменением подписки ТСП Эквайрера на сервис MirAccept

Блок 3

Новое в EMV 3DS 2.2.0

MIR Accept

Новое в спецификации EMV 3DS 2.2.0

3RI PA

платежная аутентификация в 3RI канале. Новые возможности аутентификации клиента без его присутствия при проведении платежей по подпискам и периодических платежей

Whitelistin

механизмы ведения белых списков. Дополнительная функциональность для того, чтобы сократить клиентский путь используя возможность добавления в белый список тех магазинов, которым доверяет клиент

Decoupled Authentication

отложенная аутентификация. Возможность аутентификации клиента не в процессе платежа, а позднее. В данном сценарии используется способ аутентификации вне скоупа 3DS аутентификации

3RI PA. Платежная аутентификация в 3RI канале

1

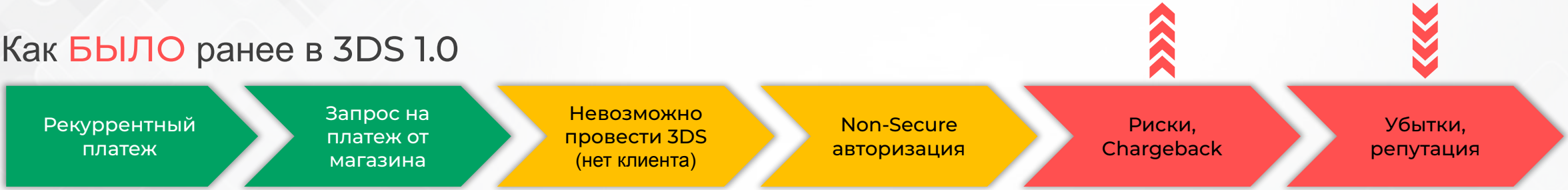
В спецификации 2.2.0 появилась возможность использовать сценарий 3RI для платежных операций (PA). Напомним, что ранее в версии 2.1.0 3RI был доступен только для не платежных операций (NPA)

Основное назначение данного вида аутентификации – это возможность получения банком Эквайрером Authentication Value при проведении платежей по подпискам и периодических платежей без присутствия клиента

2

3RI PA. Платежная аутентификация в 3RI канале

Как БЫЛО ранее в 3DS 1.0



Как СТАЛО возможно с появлением EMV 3DS 2.2.0

Основные бенефиты:

- Повышение конверсии аутентификаций в реальные авторизации
- Возможность переноса ответственности на Эмитента со стороны Эквайрера
- Снижение рисков возникновения мошеннических операций

3RI PA. Платежная аутентификация в 3RI канале

Варианты реализации

При получении банком Эмитентом подобного запроса он может выбрать, как проводить аутентификацию

Если он уверен в клиенте, либо его RBA решение оценивает операцию с низким риском – то аутентификация проходит по Frictionless пути

Если операция считается высоко рисковой, то может использоваться отложенная аутентификация (Decoupled Authentication)

Decoupled Auth. Отложенная аутентификация

В спецификации 2.2.0 стало возможно использовать так называемую отложенную аутентификацию (Decoupled Authentication). Основные отличия от стандартных сценариев EMV 3DS 2.0:

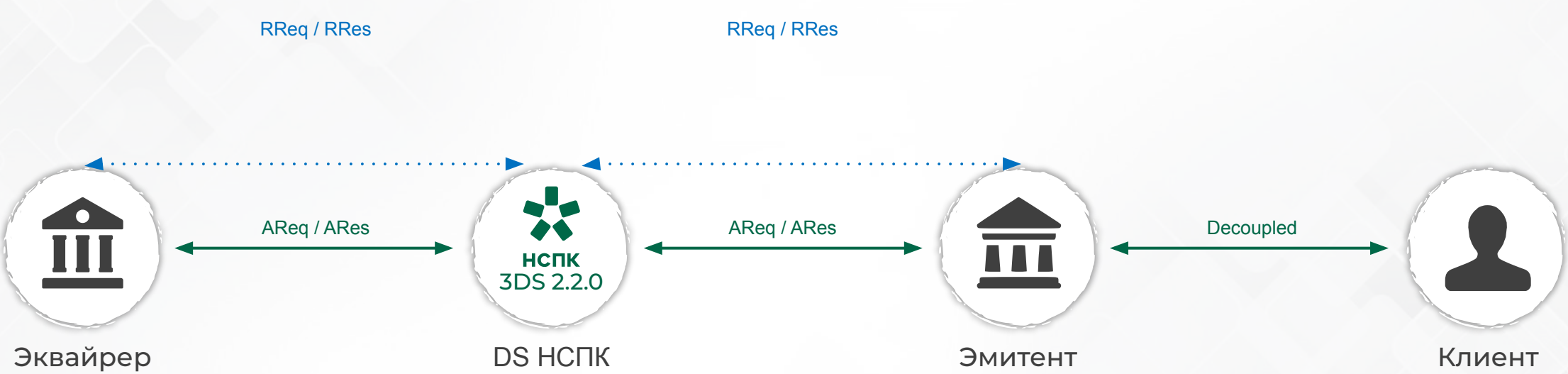
В данном типе аутентификации (Decoupled Authentication)

Отсутствуют стандартная для 2.0 протокола пара сообщений CReq / CRes

Аутентификация происходит вне скоупа 3DS аутентификации

Ожидание завершения аутентификации клиента может продолжаться до 7 дней

Decoupled Auth. Отложенная аутентификация



Decoupled Auth. Отложенная аутентификация

Бизнес применение

Данный тип аутентификации (Decoupled Authentication) может использоваться в следующих сценариях

Когда клиент в момент аутентификации не доступен, либо не может принять OTP

Когда магазин и его Эквайрер не уверены в успешном завершении конечного предоставления услуги и платеж может быть отменен

Когда банку Эмитенту необходима аутентификация клиента вне 3DS процесса, либо операция была инициирована не в сети Интернет (например: MO/TO операции)

В случае если авторизация должна пройти по карте, владелец которой отличен от того, кто проходит аутентификацию (например: использование корпоративной карты)

Whitelisting. Белые списки

Еще одно нововведение в спецификации 2.2.0.
Появился механизм ведения белых списков (Whitelisting)

Данный механизм позволяет Держателю карты, на этапе 3DS аутентификации назначить магазин в качестве доверенного, благодаря чему становится возможно сокращение клиентского пути путем проведения Frictionless

Основные бенефиты:

- Сокращение клиентского пути и как следствие увеличение лояльности клиентов
- Повышение конверсии аутентификаций в реальные авторизации

Whitelisting. Белые списки

Описание использования механизма Whitelisting

1. При проведении 3DS-аутентификации Эмитент предлагает клиенту добавить магазин в белый список
2. Клиент соглашается с предложением
3. На стороне Эмитента магазин вносится в белый список, например в виде связки к номеру карты или идентификатору клиента
4. Банк Эквайрер получает подтверждение, что магазин добавлен в белый список. Данную информацию он может сохранить у себя
5. При последующем проведении аутентификации Эквайрер может запросить возможность использования механизма Whitelisting для получения Frictionless аутентификации. При этом Эмитент также самостоятельно может принять решение об использовании Whitelisting для упрощения клиентского пути

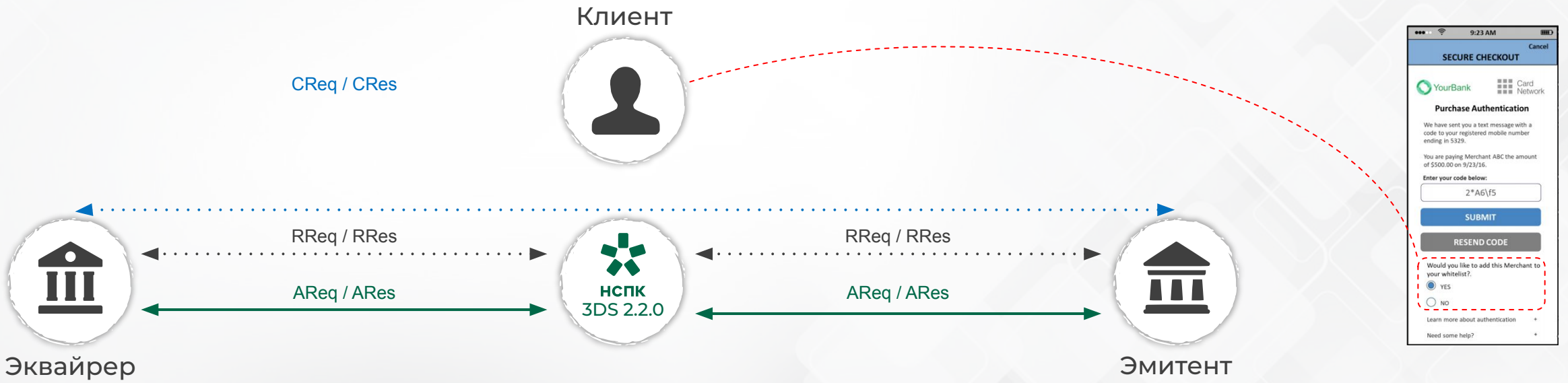
Whitelisting. Белые списки

Описание использования механизма Whitelisting

Может использоваться только в Challenge или Decoupled сценариях

Белые списки могут храниться как на стороне Эквайрера так и на стороне Эмитента

Конечное решение об использовании механизма Whitelisting принимает Эмитент при оценке риска проведения аутентификации



Документация MirAccept 2.0

Для Банков

1. Стандарт ПС «Мир». MirAccept 2.0. Руководство по внедрению для Эквайреров
2. Стандарт ПС «Мир». MirAccept 2.0. Руководство по внедрению для Эмитентов
3. Стандарт ПС «Мир». Сервис MirAccept. Руководство по проведению тестовых испытаний подключения к сервису для Участников и Вендоров
4. Руководство по оформлению зон обслуживания карты Мир в среде Интернет
5. Регламент оказания услуг Удостоверяющего центра АО «НСПК» в рамках предоставления платежных сервисов
6. Реестр одобренных вендоров MirAccept

Для Вендоров

Стандарт платежной системы «Мир». Сервис MirAccept. Руководство по проведению тестовых испытаний подключения к сервису для Участников и Вендоров

Спасибо за внимание!!!

Ковачев Виталий
Главный технический администратор Платформы
3-D Secure
Операционно-технологический
Департамент АО «НСПК»
kovachevvy@nspk.ru