SmartBanking

# Описание процессов и архитектуры решения SmartBanking Access Control Server (sbACS)

Москва, 2024

# Отказ от ответственности

Здесь и далее, название АЦС, как и другие англицизмы, продиктованы исключительно общепринятой терминологией в данной бизнес-области и употребляются для упрощения понимания функционала и спецификации EMV.

АЦС является транслитерацией от акронима ACS на английском языке. Которая, в свою очередь, означает Access Control Server. На русском языке данное название имеет перевод как Сервер Контроля Доступа (СКД). По всем дальнейшим сокращениям и терминологии необходимо обращаться к разделу Акронимы и Терминология.

# Кратко о Продукте

Access Control Server компании Smart Banking предназначен для эмитентов, участвующих в программах 3-D Secure международных платежных сетей.

Решение поддерживает регистрацию карт, аутентификацию запросов на совершение операций и уведомление владельцев карт.

sbACS представляет собой систему с несколькими эмитентами и позволяет банкам-эмитентам настраивать каждый параметр для конкретного индивидуального профиля.

Он поддерживает аутентификацию на основе риска (RBA), которая помогает эмитенту сократить число случаев отмены транзакций, внешнюю аутентификацию (OOB), которая повышает удобство работы пользователей и делает платежи удобными, а также множество стандартных и настраиваемых методов аутентификации, таких как OTP (любой канал доставки, как смс, электронная почта, push) и многое другое.

# СОДЕРЖАНИЕ

# Акронимы и Терминология

| Термин | Акроним | Описание |
|---|---|---|
| 3DS Server | 3DSS | Компонент Домена Эквайрера, который обеспечивает взаимодействие между средой 3DS Requestor Environment и компонентом DS для аутентификации Держателя карты.<br>Компонент 3DS Server отвечает за:<br>• сбор необходимых элементов данных для сообщений протокола EMV 3-D Secure;<br>• аутентификацию компонента DS;<br>• валидацию компонента DS, компонента 3DS SDK и компонента 3DS Requestor;<br>• обеспечение защиты содержания сообщений. |
| 3-D Secure Software Development Kit | 3DS SDK | Компонент, который встроен в 3DS Requestor App (приложение ТСП, установленное на средстве персональной коммуникации Держателя карты). |
| 3DS Requestor Initiated | 3RI | Подтверждение платежного средства Эмитентом, инициированное ТСП электронной коммерции или его сервис провайдером, которое выполняется без непосредственного участия в этом процессе Держателя карты. |
| Access Control Server | ACS | Компонент Домена Эмитента, который взаимодействует с инфраструктурой MirAccept, проверяет, доступна ли аутентификация для номера карты и типа устройства, а также аутентифицирует Держателя карты. |
| Directory Server | DS | Компонент Домена платежной системы, выполняющий ряд функций, включая маршрутизацию аутентификационных сообщений и аутентификацию серверов в Доменах Эквайрера и Эмитента. |
| 3-D Secure | 3DS | Совокупность открытых спецификаций протокола надежной аутентификации Держателя карты при проведении операции в сети Интернет, разработанных EMVCo. Термин может использоваться в сочетании с мажорными версиями спецификации 2.1.0 и 2.2.0. |
| EMVCo | EMVCo | Организация, способствующая разработке стандартов в области платежных технологий. |
| Сервис-провайдер (Internet Payment Service Provider) | IPSP | Сторонняя организация, привлеченная Участником с целью обеспечения взаимодействия с Операционным центром ПС для оказания Участнику услуг по |

| | | |
|---|---|---|
| | | аутентификации Держателей карт при выполнении Операций в сети Интернет с использованием технологии надежной аутентификации. Организация, выполняющая функции IPSP, должна иметь действующий сертификат соответствия требованиям Стандарта PCI DSS. |
| **Сертификат** | | Электронный документ, выданный УЦ ПС. Здесь и далее под сертификатом понимается не являющийся квалифицированным сертификат ключа проверки электронной подписи формата X.509 v.3 (https://tools.ietf.org/html/rfc5280), содержащий открытый ключ владельца, идентификатор владельца, срок действия сертификата, условия использования закрытого ключа, соответствующего сертификату, идентификатор УЦ. |
| **Удостоверяющий центр Certificate Authority** | УЦ CA | Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, выполняющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». |
| **3DS Requestor** | | Инициатор запроса аутентификации EMV 3-D Secure. Например, это может быть продавец или цифровой кошелек, запрашивающий аутентификацию внутри потока покупок. |
| **3DS Method** | | Вызов сценария, предоставляемый интегратором 3DS и размещаемый на сайте 3DS Requestor. Опционально используется для получения дополнительной информации о браузере держателя карты, для облегчения принятия решений, основанных на риске. |
| **Authentication** | | В контексте 3-D Secure, процесс подтверждения того, что человек, совершая транзакцию электронной коммерции, имеет право использовать платежную карту. |
| **Authentication Value** | AV | Криптографическое значение, генерируемое ACS, для обеспечения возможности проверки авторизационной системой целостности результата аутентификации. Алгоритм AV определяется каждой Платежной системой. |
| **Authorisation** | | Процесс, посредством которого Эмитент или обработчик от имени Эмитента, утверждает транзакцию к оплате. |
| **Authorisation System** | | Системы и услуги, посредством которых Платежная система осуществляет свою деятельность: онлайн- услуги финансовой |

| | | |
|---|---|---|
| | | обработки, авторизации, клиринга и расчетов эмитентам и эквайерам. |
| **Bank Identification Number** | BIN | Первые шесть или восемь цифр номера платежной карты, которые однозначно идентифицируют финансовое учреждение-эмитент. |
| **Base64** | | Кодирование, применяемое к элементу данных «Authentication Value», как определено в RFC 2045. |
| **Base64url** | | Кодирование, применяемое к данным 3DS Method Data, Device Information и сообщениям CReq/CRes, как определено в RFC 7515. |
| **Cardholder** | | Физическое лицо, которому выдана карта или которое имеет право ее использовать. |
| **Challenge Flow** | | Поток 3-D Secure, включающий взаимодействие с держателем карты. |
| **Electronic Commerce Indicator** | ECI | Значение, специфичное для платежной системы, предоставляемое ACS для обозначения результатов аутентификации держателя карты. |
| **Frictionless Flow** | | Поток 3-D Secure, который не предполагает взаимодействия с держателем карты. |
| **One-Time Passcode** | OTP | Код доступа, действительный только для одной попытки аутентификации. |
| **Out-of-Band** | OOB | Процесс аутентификации, выполняемый вне основного потока, но параллельно с ним. Последний запрос не используется для передачи данных в ACS, но сигнализирует только о том, что аутентификация завершена. Методы аутентификации не определяются спецификацией 3-D Secure. |
| **Payment System** | PS<br>IPS | Платежная система, определяющая правила и условия работы, а также требования к выпуску карты и приему торговцами. |
| **Whitelisting** | | Процесс ACS, позволяющий держателю карты поместить запрашивающую сторону 3DS в список доверенных бенефициаров. |

# Описание Продукта

sbACS — это программное решение для эмитентов платежных карт, позволяющее безопасно аутентифицировать транзакции без предъявления карты (CNP) через Интернет.

Решение поддерживает регистрацию карт, аутентификацию запросов на оплату и уведомление владельцев карт.

## Версия 3-D Secure

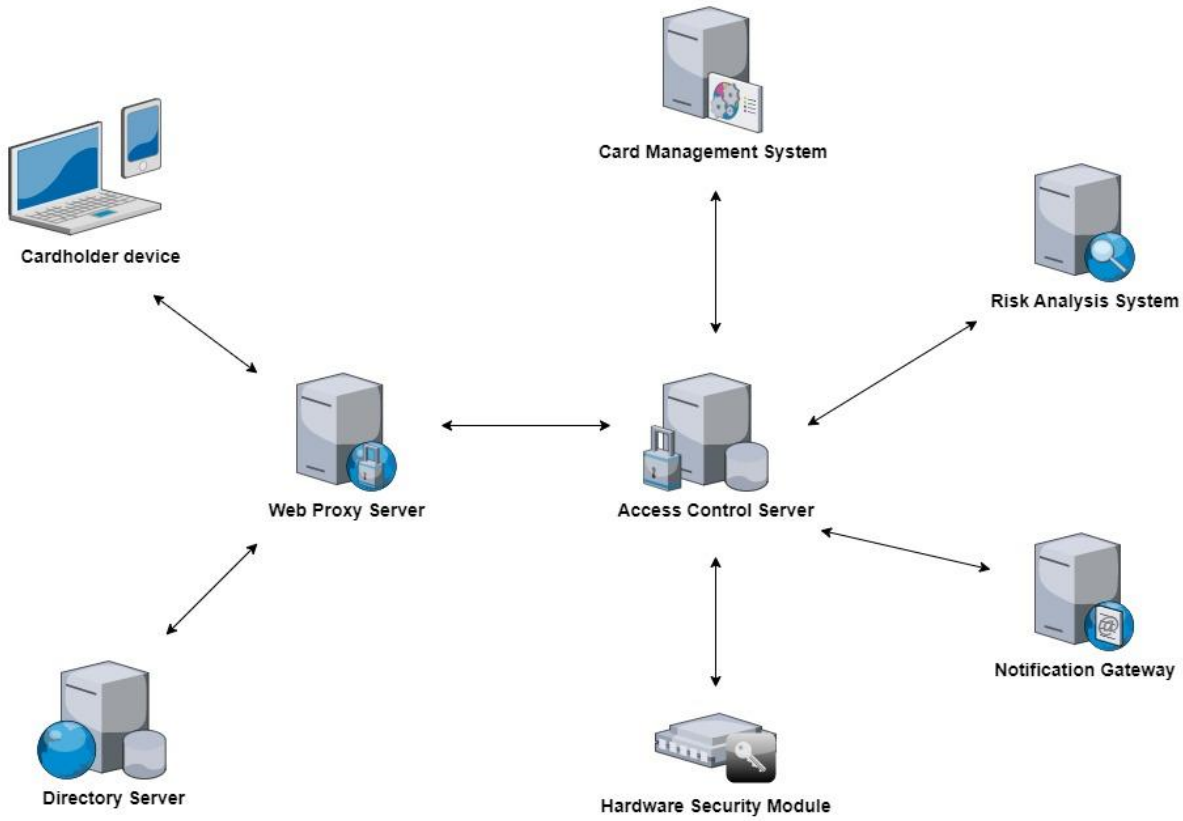
Если вы не знакомы с технологией 3-D Secure, ознакомьтесь со спецификацией протокола EMV 3-D Secure и основных функций (https://www.emvco.com/specifications/emv-3-d-secure-protocol-and-core-functions-specification-2/).

Поддерживаемая версия протокола 3-D Secure — 2.2.0

## Поддерживаемые программы платёжных систем

- Mastercard Identity Check
- Visa Secure
- НСПК MirAccept
- UnionPay 3-D Secure
- Discover Diners ProtectBuy

## Архитектура решения




Основная идея, которую необходимо осознать, заключается в том, что ACS является центром многочисленных интеграций.

В зависимости от требований проекта, ACS может быть интегрирован со следующими системами:

*CMS (Card Management System)* – место хранения карт. В качестве CMS может использоваться система OLTP (онлайн-обработка транзакций). Также возможно сохранение карточек в БД ACS.

*RAS (Система анализа рисков)* — система предотвращения мошенничества, необходимая для выполнения RBA (Аутентификация на основе рисков).

*NG (Notification Gateway)* – система, которая отправляет владельцу карты SMS с OTP (одноразовым паролем).

*HSM (Аппаратный модуль безопасности)* — аппаратный сервер, который необходим для расчета AV (значения

аутентификации), основной цели функциональности 3-D Secure. Некоторым проектам для поддержки этой функциональности требуется дополнительная интеграция с OLTP, без прямой связи между ACS и HSM.

*DS (сервер каталогов)* — сервер платежной схемы (PS) для выполнения 3DS, являющийся частью общей инфраструктуры 3DS. Соединение с DS устанавливается обычным способом через реверсивный прокси-сервер (типа nginx или аналогичный), поскольку для этого необходимы сертификаты, подписанные PS, размещенные на прокси. Но возможно установить соединение и с самого АЦС.

*Устройства держателя карты* – это может быть браузер или мобильное устройство, соединение устанавливается так же, как и для DS, но с соответствующими сертификатами.

## Аутентификация плательщика

sbACS поддерживает следующие методы аутентификации плательщика:

- ОТП

*Код доступа, действительный только для одной попытки в рамках платежа. Владелец карты может получить его по SMS, push-уведомлению или по электронной почте.*

- Статический пароль

*Как следует из названия, статический пароль представляет собой неизменную строку символов, очень похожую на пароли, которые плательщик создаёт для различных учетных записей в Интернете.*

- Риск-ориентированный

*RBA напрямую связан с «Frictionless Flow» и не требует дальнейшего взаимодействия с держателем карты для достижения успешного результата аутентификации.*

- Внешняя аутентификация

*Взаимодействие с держателем карты, которое выполняется вне потока 3-D Secure, но параллельно с ним. Методы или реализации аутентификации не определены спецификацией 3-D Secure. Одним из возможных методов аутентификации, может быть, использование биометрических данных.*

- Неплатежная аутентификация

*Проверка личности и подтверждение аккаунта. Может использоваться для регистрации карты в кошельке, оплаты счетов без участия владельца карты и т. д.*

### Аутентификация на основе рисков

Аутентификация на основе рисков (RBA) требует интеграции с внешней системой анализа рисков (RAS).
Взаимодействие интегрированных систем выглядит следующим образом:

- ACS отправляет в систему анализа рисков запрос, содержащий AReq и BrowseInfo.
- Основываясь на своей собственной логике, RAS выбирает, какой тип аутентификации применить: «Frictionless» или «Challenge», и отправляет ответ в ACS, в противном случае RAS советует ACS отклонить транзакцию.

Ответ системы анализа рисков содержит следующие параметры:

- Рекомендация по типу аутентификации, применяемому к транзакции – «Frictionless», «Challenge» или «Reject»;
- Рассчитанная величина риска;
- Схема аутентификации, которая будет применяться для вызова.

- В зависимости от своих настроек, ACS использует один из параметров, предоставленных RAS, для определения типа аутентификации. В случае расчёта риска, пороговое значение необходимо настроить в ACS на уровне системы или

профиля.

- После определения типа аутентификации ACS продолжает работу и отправляет в систему анализа рисков уведомление с информацией о завершении аутентификации. Это уведомление содержит threeDSServerTransID (в качестве идентификатора транзакции) и статус операции.

- Когда RAS рекомендует схему аутентификации, которая должна применяться для проверки держателя карты, ACS должен сообщить RAS о конкретном методе(ах) аутентификации, который был выполнен.

### Внешняя аутентификация

Примером внешней аутентификации (OOB) может быть push-уведомление банковскому приложению, которое завершает аутентификацию и затем отправляет результаты в ACS. Другим вариантом аутентификации OOB могут быть биометрические данные.

ACS инициирует внешнее взаимодействие с держателем карты, а не взаимодействует с держателем карты через 3DS SDK.

- Информация о вызове в сообщении CRes состоит только из инструкций для держателя карты о том, как выполнить аутентификацию OOB.

- ACS получает подтверждение о том, что Держатель карты выполнил аутентификацию OOB.

Алгоритм принятия решения об аутентификации для OOB зависит от реализации, однако ACS необходим доступ к результату аутентификации OOB.

### Неплатежная аутентификация

Неплатежная аутентификация (NPA) — это транзакция 3-D Secure, инициированная запрашивающей стороной для подтверждения действительности учетной записи. В основном она используется для повторяющихся транзакций (подписка на

телевидение, оплата счетов за коммунальные услуги и т. д.), когда продавцу необходимо убедиться, что пользователь подписки по-прежнему способен осуществлять данный платеж.

В рамках транзакции 3DS, инициированной запрашивающей стороной (3RI), ACS определяет, доступна ли аутентификация для держателя карты, используя номер карты из сообщения AReq.

Если аутентификация недоступна для данного номера карты, ACS возвращает на сервер 3DS сообщение ARes со статусом транзакции и кодом причины статуса транзакции, установленным в соответствующий ответ, как определено конкретным DS, и завершает обработку.

В остальных случаях ACS возвращает ARes с соответствующими данными согласно спецификации EMV 3DS.

## Управление сертификатами

Сертификаты используются в следующих целях:

- Безопасное соединение с участниками 3-D Secure (TLS)
- Подключение клиента 3DS к ACS (взаимодействие Challenge)
- Соединение браузера с ACS (для 3DS Метода)

## Взаимодействие с HSM

HSM используется для генерации криптографических значений для аутентификации в рамках операции, требуемой спецификацией EMV 3DS.

Поддерживаются следующие модели HSM:

- Thales payShield 10000, 9000

## Взаимодействие со шлюзом уведомлений

ACS может использовать сторонний шлюз уведомлений для доставки SMS, электронной почты или push-уведомлений в рамках Challenge или другого процесса уведомления.

Уведомительные сообщения генерируются на основе предопределенных шаблонов.

## PCI DSS compliance

Компания Smart Banking гарантирует безопасность своего продукта sbACS и соответствие международным стандартам PCI 3DS и PCI DSS.

## Метрики

Метрики — это количественные показатели событий в системе.

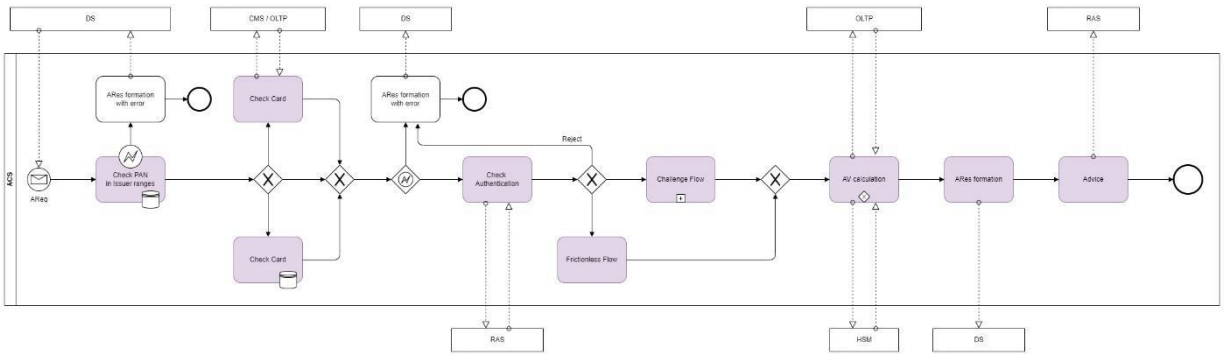
Метрики можно использовать для мониторинга и анализа доступности и производительности системы.

sbACS предоставляет всю необходимую информацию и данные для мониторинга таким популярным инструментам, как Prometheus и Grafana, в качестве графического интерфейса и инструмента отчетности.

## Технологический стек

OpenJDK, PostgreSQL

# Описание процессов




● AReq поступает от DS в результате запроса владельца карты на совершение транзакции.

● ACS должен проверить PAN из AReq, чтобы убедиться, что он относится к диапазонам эмитента, иначе процесс завершится с ошибкой.

● Следующий шаг необходимо разделить на три отдельных процесса. Для каждого конкретного профиля выполняется только один из них:

- Карта проверена в БД СКУД.
- Карта проверена в OLTP/CMS.
- Карта вообще не проверяется на этом этапе, и контроль проверки осуществляется на RAS.

● Во всех трех случаях валидация завершается дополнительной проверкой услуги 3DS, статуса блокировки карты, недостаточности средств и так далее.

● Независимо от того, какая система была выбрана для проверки карты, если валидация дала отрицательный результат, процесс завершается с ошибкой.

● В противном случае аутентификация должна быть подтверждена в RAS. Существует два варианта того, как RAS предоставляет результат проверки:

- Результат содержит информацию только о самом решении по аутентификации, если оно будет отклонено, о подтверждении аутентификации (frictionless flow) или о вызове аутентификации держателя карты для будущего запроса авторизации (challenge flow).
- RAS может сообщить ACS, какой список методов аутентификации будет использоваться.

- В зависимости от того, какой ответ получен от RAS, применяется один из следующих потоков:

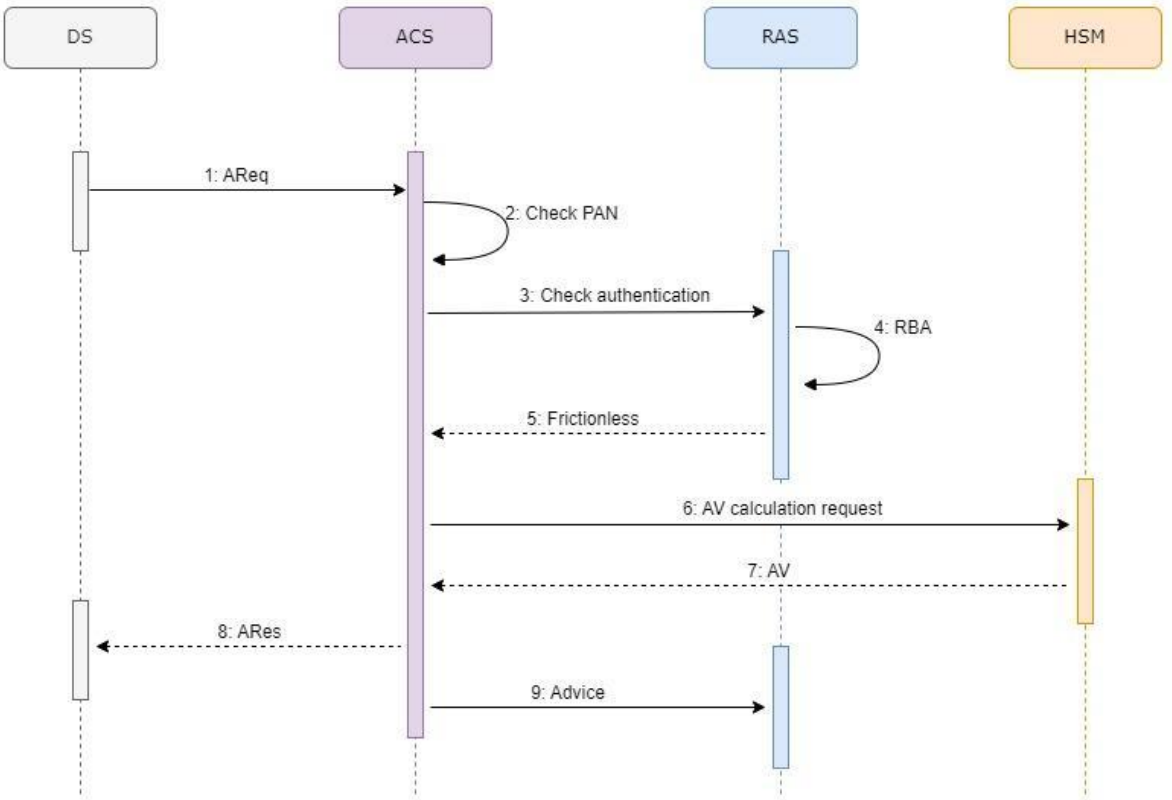
- Frictionless Flow
- Challenge Flow
- Отклонить, процесс завершен с ошибкой (Reject)

- Если аутентификация выполнена успешно, ACS должен предоставить продавцу AV результат, сгенерированный через HSM или OLTP.

- После расчета AV ACS отправляет ARes/RReq обратно в DS.

- Последний шаг (необязательный) — уведомление RAS о результате аутентификации.

## Frictionless Flow



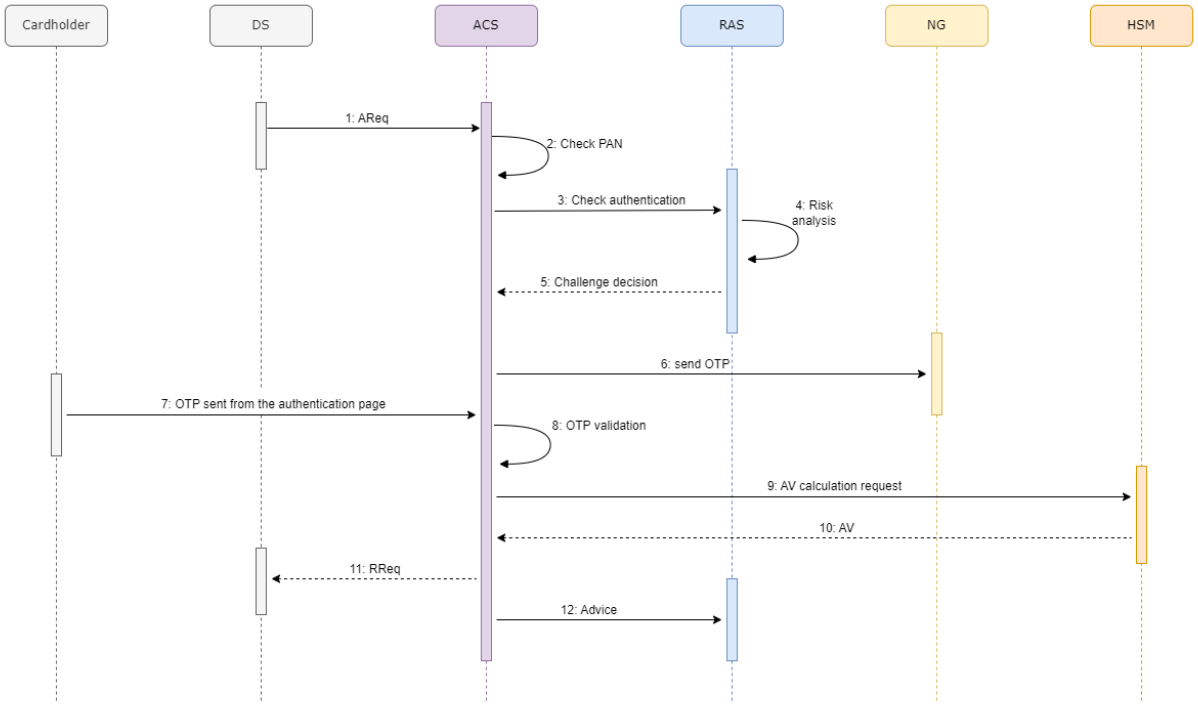

- В среде, в которой происходит платёж, необходимая информация 3-D Secure собирается и передается на сервер 3DS (3DSS) для включения в сообщение AReq. Используя информацию, предоставленную владельцем карты, и данные, собранные в среде, где происходит платёж, сервер 3DS создает и отправляет сообщение AReq на DS, который затем пересылает это сообщение в соответствующий ACS.

- ACS оценивает данные, предоставленные в сообщении AReq. В ходе Frictionless Flow ACS определяет, что дальнейшее взаимодействие с держателем карты не требуется для завершения аутентификации.

- В ответ на сообщение AReq ACS возвращает сообщение ARes на DS, который затем пересылает это сообщение инициирующему 3DS-серверу. Сервер 3DS передает результат сообщения ARes в среду запроса 3DS, которая затем информирует об этом держателя карты.

## Challenge Flow

Схема потока запроса изображена ниже на основе метода аутентификации SMS OTP и потока на основе браузера.




- То же, что и «Frictionless Flow», за исключением того, что сообщение ARes указывает, что для завершения аутентификации требуется дальнейшее взаимодействие с держателем карты.

- Клиент 3DS инициирует сообщение CReq на основе информации, полученной в сообщении ARes. Способ, которым это делается, зависит от модели:

  - На основе приложения — сообщение CReq формируется 3DS SDK и отправляется по URL-адресу ACS, полученному из сообщения ARes.
  - На основе браузера — сообщение CReq формируется сервером 3DS и отправляется через браузер держателя карты на URL-адрес ACS, полученный из сообщения ARes.

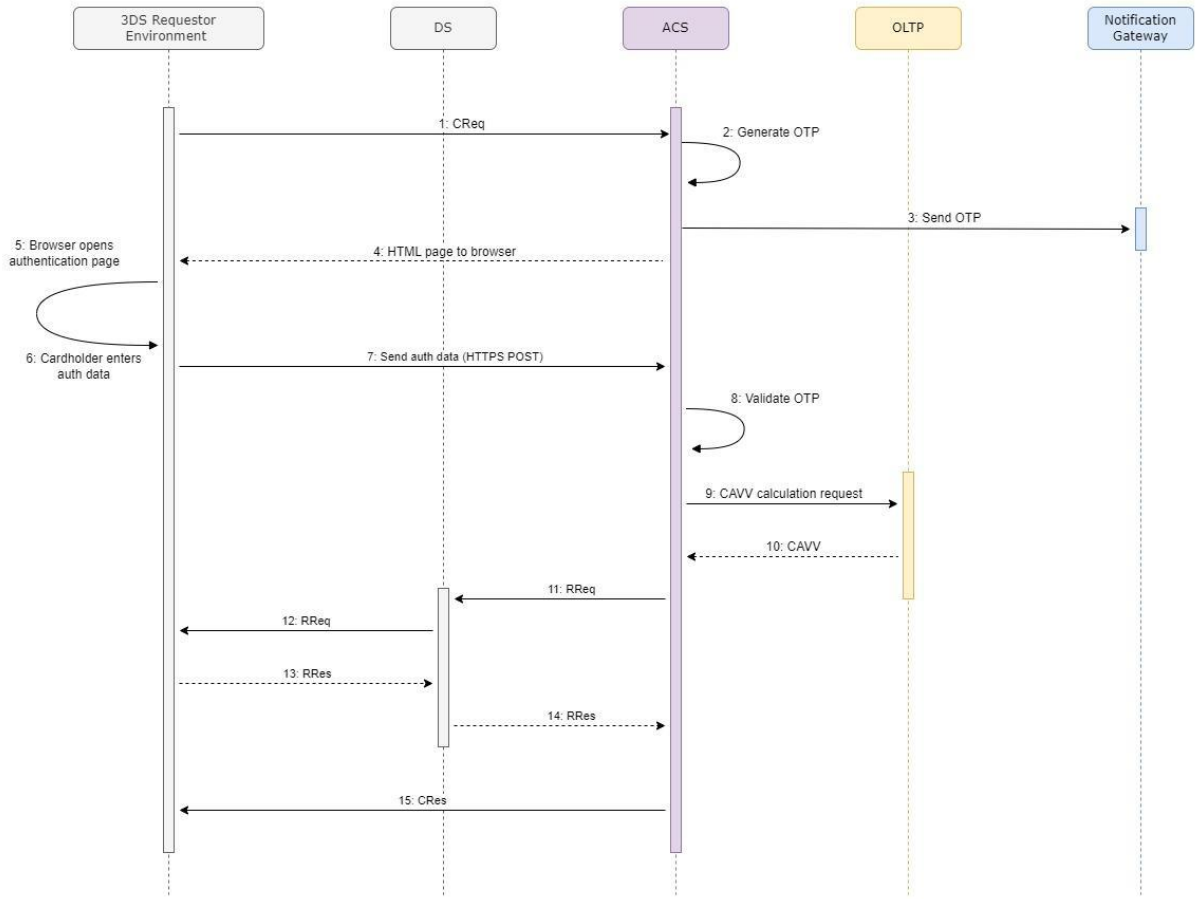
- ACS получает сообщение CReq и взаимодействует с держателем карты. ACS отправляет пользовательский интерфейс аутентификации (страницу HTML) в браузер держателя карты (на основе браузера). Владелец карты вводит данные аутентификации через браузер для проверки ACS.

Для приложений процесс немного отличается. Подробности см. в спецификации EMV.

- В ответ на сообщение CReq ACS формирует сообщение CRes и отправляет его на 3DS-сервер для указания результата аутентификации.

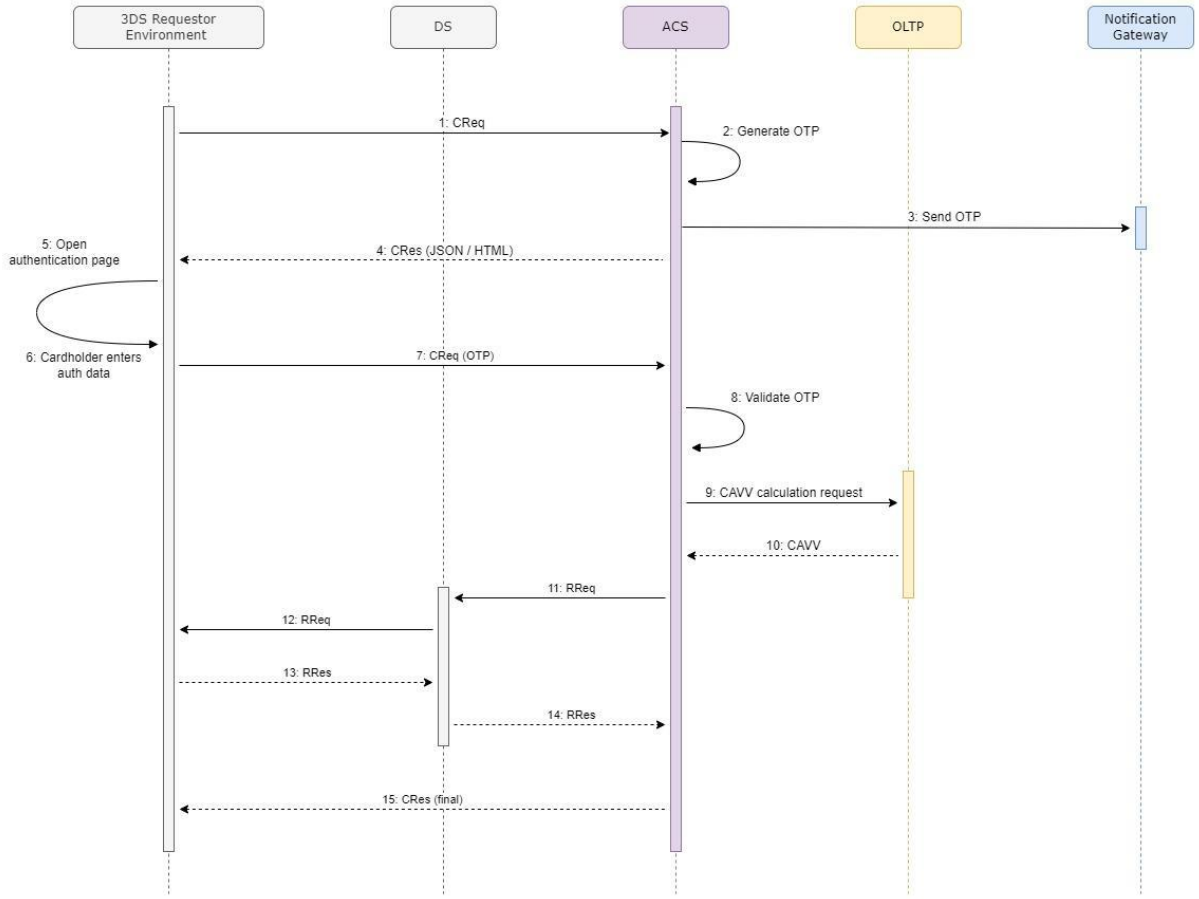
## Потоки на основе браузера и приложения

На следующих диаграммах поясняются различия между потоками на основе браузера и приложения с точки зрения взаимодействия.




Основное отличие потока браузера заключается в том, что обмен сообщениями CReq/CRes выполняется только один раз. И окончательный CRes является единственным результатом аутентификации, который браузер получает от эмитента. Сообщения CReq/CRes больше не допускаются!

В то время как для приложений это цикл, и взаимодействие CReq/CRes может выполняться несколько раз, пока не будет достигнут результат аутентификации.




Кроме того, вы должны понимать разницу в пользовательском интерфейсе. Запрос платежа с мобильного устройства не означает использование приложения!

С точки зрения торгового приложения, особенностью реализации пользовательского интерфейса является поддержка встроенных элементов управления для Android/iOS. И только этот конкретный случай должен быть обработан как приложение, и предусмотрены соответствующие индикаторы.

# Условия использования

## Аппаратное обеспечение

минимум: 4 ядра процессора i3, 8 ГБ ОЗУ, 50 ГБ жесткого диска
средний: 4–8 процессорных ядер i5, 8–16 ГБ ОЗУ, 50–100 ГБ HDD/SSD
максимум: 8 процессорных ядер i7, 16 ГБ ОЗУ, 100 ГБ SSD

## Среда

Предусмотрено несколько вариантов развертывания ACS:

- Автономный

Для установки в автономном режиме требуется только Java (не ниже 11-ой версии).

- Docker-Compose

Docker и Docker Compose должны быть установлены предварительно.

## База данных

Для базы данных необходима единственная пустая схема, все необходимые объекты создаются Flywaydb в процессе развертывания.

Поддерживаются следующие версии баз данных:

- PostgreSQL 9.6+

## Система

ACS поставляется как автономное приложение, которое имеет небольшой вес и не требует отдельного сервера приложений.