SmartBanking

Описание функциональных характеристик 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. Компонент 3DS Server отвечает за: • сбор необходимых элементов данных для сообщений протокола EMV 3-D Secure; • аутентификацию компонента DS; • валидацию компонента DS, компонента 3DS SDK и компонента 3DS Requestor; • 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 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.

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 2.

Спецификации

Данный раздел предназначен для технических специалистов, которым необходимо интегрировать внешние системы с сервером контроля доступа ACS. В документе описан полный набор параметров, участвующих в передаче данных между системами в рамках интеграции с ACS.
Для описания формата полей используются следующие соглашения:

- 9 – фиксированная длина поля данных;
- 9..99 – минимальная и максимальная длина поля с переменной длиной данных;
- ANS – буквенные, цифровые и специальные символы;
- N – десятичные цифры;
- LZP – дополненный левыми нулями;
- UUID – универсальный уникальный идентификатор.

ACS будет отправлять сообщения через HTTP с запросом POST на указанный URL-адрес.
JSON необходимо использовать в качестве формата данных для передачи данных между системами.

Интеграция со Шлюзом Уведомлений

Send

Параметры запроса

Имя параметра	Формат данных	Обязательный	Описание
channel	A 3..5	Обязательный	Возможные значения: - SMS - EMAIL - PUSH
text	Строка	Обязательный	Текст сообщения
messageId	Строка	Опциональный	Идентификатор сообщения.
phone	Строка вида \+?[0-9]	Условный	Номер телефона, на который необходимо отправить сообщение.
email	Строка вида [@]+@[\.]+\..+	Условный	Электронная почта, на которую необходимо отправить сообщение.
pushId	ANS ..200	Условный	Push ID, на который необходимо отправить сообщение.
title	Строка	Условный	Заголовок для push уведомления.
pan	N16..19	Опциональный	Номер карты.
externalCardId	ANS 1..256	Опциональный	Идентификатор карты во внешней системе.
externalCustomerId	ANS 1..256	Опциональный	Идентификатор держателя карты во внешней системе.
languageTag	A2	Опциональный	Язык, с которым необходимо отправить уведомление.

Параметры ответа

ACS не ожидает никакого ответа, кроме кодов состояния HTTP.

Интеграция с внешней системой Аутентификации

Аутентификация OOB — это процесс аутентификации плательщика, который выполняется вне основного потока аутентификации. Примером OOB-аутентификации является случай, когда ACS отображает плательщику сообщение с инструкцией открыть мобильное приложение для подтверждения покупки. Ещё вариант OOB аутентификации — это биометрия.

Start Authentication

Сообщение «Start Authentication» используется для инициализации процесса аутентификации в системе OOB.

Параметры запроса

Имя параметра	Формат данных	Обязательный	Описание
transactionId	UUID	Обязательный	Идентификатор транзакции 3DS-сервера
accountNumber	N 13..19	Условный	Номер карты. Должно присутствовать одно из следующих трех значений: ● номер счета ● ID карты ● хэш номера карты
cardID	ANS 1..32	Условный	Идентификатор карты во внешней системе. Должно присутствовать одно из

			следующих трех значений: • номер счета • ID карты • хэш номера карты
accountNumberHash	ANS 1..128	Условный	Значение хеша PAN в формате Base64 с алгоритмом SHA-2 256. Должно присутствовать одно из следующих трех значений: • номер счета • ID карты • хэш номера карты
displayedAccountNumber	N4	Опциональный	Представление PAN, которое безопасно отображать в пользовательском интерфейсе. Например, 4 последние цифры PAN.
network	String	Опциональный	Название платёжной сети.
authenticationRequestData	ANS	Опциональный	Данные, которые могут потребоваться для аутентификации на основе сообщения AReq. Структура JSON используется для указания каждого

			конкретного поля. Следующие три параметра включены в массив JSON.
{			
purchaseDate	N14 YYYYMMDDHHmmSS	Опциональный	Дата и время покупки, выраженные в формате UTC.
acquirerMerchantID	ANS 1..35	Опциональный	Идентификатор продавца, присвоенный эквайером.
threeDSRequestorURL	ANS 1..2048	Опциональный	Полный URL-адрес веб-сайта запрашивающего 3DS
}			
destination	ANS 1..256	Условный	Адрес доставки одноразового пароля (OTP), например номер телефона или адрес электронной почты.
amount	N 1..48	Обязательный	Сумма операции в минимальных единицах валюты со всеми удаленными разделителями.
currency	N 3 LZP	Обязательный	Валюта операции.
merchantName	ANS 1..40	Обязательный	Имя продавца.
authenticationMethod	N2	Опциональный	Метод аутентификации,

			назначенный карте в ACS, принимаемые значения параметров и их значения определены в спецификации протокола EMV 3-D Secure. Допустимые значения: 01–10 80–99
externalCustomerId	ANS 1..32	Опциональный	Идентификатор клиента во внешней системе.
callbackURL	ANS 1..2048	Условный	URL-адрес конечной точки получения результата аутентификации, куда ACS будет получать информацию о результате аутентификации из системы OOB.

Параметры ответа

Имя параметра	Формат данных	Обязательный	Описание
transactionId	UUID	Обязательный	Идентификатор транзакции 3DS-сервера
authenticationId	UUID	Условный	Идентификатор аутентификации, полученный от системы аутентификации.

			В случае ошибки это поле отсутствует.
authenticationMethod	N2	Опциональный	Метод аутентификации, назначенный карте в ACS, принимаемые значения параметров и их значения определены в спецификации протокола EMV 3-D Secure. Допустимые значения: 01–10 80–99
sessionExpirationDate	N 14 YYYYMMDDHHmmSS	Опциональный	Дата окончания сеанса аутентификации в формате UTC.
errorCode	Единственное возможное значение — 1 (числовое).	Условный	Код ошибки предоставлен внешней системой. Если, по какой-либо причине, при обработке запроса произошла ошибка, это поле является обязательным.
errorDescription	ANS 1..200	Условный	Описание ошибки, предоставленное внешней системой.

Obtain Authentication Result

Сервис используется для получения результата процесса аутентификации из системы OOB.

Параметры запроса

Имя параметра	Формат данных	Обязательный	Описание
transactionId	UUID	Обязательный	Идентификатор транзакции 3DS-сервера
authenticationId	UUID	Условный	Идентификатор аутентификации, полученный от системы аутентификации. В случае ошибки это поле отсутствует.
authenticationResult	Строка	Обязательный	Допустимые значения: OK – аутентификация прошла успешно и ACS может продолжать работу; FAILED_ATTEMPT – попытка аутентификации не удалась, плательщик может выполнить попытку аутентификации еще раз; FAILED – аутентификация не удалась; NOT_FINISHED - плательщик проходит аутентификацию, ACS ожидает результата; ОШИБКА - ошибка системы аутентификации, ACS прекращает обработку.

authenticationMethod	N2	Опциональный	Метод аутентификации, назначенный карте в ACS, принимаемые значения параметров и их значения определены в спецификации протокола EMV 3-D Secure. Допустимые значения: 01–10 80–99
resultReason	ANS 1..1000	Опциональный	Описание результата аутентификации.
enteredPassword	ANS 1..64	Опциональный	Пароль, введенный плательщиком для метода аутентификации на основе пароля.

Параметры ответа

ACS не ожидает никакого ответа, кроме кодов состояния HTTP.

Get Authentication Result

Сообщение используется для получения результата процесса аутентификации из системы OOB.

Параметры запроса

Имя параметра	Формат данных	Обязательный	Описание
transactionId	UUID	Обязательный	Идентификатор транзакции 3DS-сервера
authenticationId	UUID	Условный	Идентификатор аутентификации, полученный от системы аутентификации. В случае ошибки это поле отсутствует.

enteredPassword	ANS 1..64	Опциональный	Пароль, введенный плательщиком для метода аутентификации на основе пароля.

Параметры ответа

Имя параметра	Формат данных	Обязательный	Описание
transactionId	UUID	Обязательный	Идентификатор транзакции 3DS-сервера
authenticationId	UUID	Условный	Идентификатор аутентификации, полученный от системы аутентификации. В случае ошибки это поле отсутствует.
authenticationResult	Строка	Обязательный	Допустимые значения: OK – аутентификация прошла успешно и ACS может продолжать работу; FAILED_ATTEMPT – попытка аутентификации не удалась, плательщик может выполнить попытку аутентификации еще раз; FAILED – аутентификация не удалась; NOT_FINISHED - плательщик проходит аутентификацию, ACS ожидает результата; ОШИБКА - ошибка системы аутентификации, ACS прекращает обработку.

authenticationMethod	N2	Опциональный	Метод аутентификации, назначенный карте в ACS, принимаемые значения параметров и их значения определены в спецификации протокола EMV 3-D Secure. Допустимые значения: 01–10 80–99
resultReason	ANS 1..1000	Опциональный	Описание результата аутентификации.
enteredPassword	ANS 1..64	Опциональный	Пароль, введенный плательщиком для метода аутентификации на основе пароля.

Интеграция с Системой анализа риска

Check authentication

Параметры запроса

Имя параметра	Формат данных	Обязательный	Описание
areq	См. B.1 в спецификации протокола EMV 3-D Secure.	Обязательный	Сообщение AReq согласно спецификации 3DS2.
browserInfo	JSON object	Опциональный	Объект JSON содержащий поля браузера, необходимые для формирования AReq и получаемые ACS непосредственно из браузера клиента.

Параметры ответа

Имя параметра	Формат данных	Обязательный	Описание
respCode	N1	Условный	Возможны следующие значения: 1 – Frictionless 0 – Challenge -1 – Reject Должен быть указан только один параметр respCode или risk.
risk	N3	Условный	Целочисленное значение порога, рассчитанное системой риска. Должен быть указан только один параметр respCode или risk.
authenticationSchema	AN	Условный	Имя схемы аутентификации, предопределенное в ACS, которое рекомендуется применять для вызова.
additionalData	JSON object	Опциональный	Любая дополнительная информация, необходимая в рамках сообщения. Поддерживается шаблон «ключ-значение». Например, когда схема аутентификации рассматривает проверку OTP, необходимо указать номер телефона (электронную почту

			или идентификатор push-уведомления). Возможные значения ключа: **phone** **email** **pushId** Уведомление будет предоставлено клиенту для каждого канала доставки, полученного в этом параметре.

Advice

Параметры запроса

Имя параметра	Формат данных	Обязательный	Описание
threeDSServerTransID	UUID	Обязательный	Должно быть то же значение, что и в AReq
operationStatus	A1..2	Обязательный	Текущий статус операции со следующими возможными значениями: AF - аутентифицированный, поток Frictionless AC – аутентифицированный, поток Challenge AD – аутентифицированный, поток Decoupled FF — аутентификация не удалась, поток Frictionless FC — аутентификация не удалась, поток Challenge

			FD – аутентификация не удалась, поток Decoupled C – отменено A – заброшенный E – ошибка
authenticationMethod	N2	Опциональный	Метод аутентификации, назначенный карте в ACS, принимаемые значения параметров и их значения определены в спецификации протокола EMV 3-D Secure. Допустимые значения: 01–10 80–99

Параметры ответа

ACS не ожидает никакого ответа, кроме кодов состояния HTTP.