SmartBanking

Техническая поддержка программного обеспечения 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.

Техническая поддержка программного обеспечения

При возникновении каких-либо вопросов или сбоев необходимо обратиться в Службу поддержки программных продуктов ООО «СмартБанкинг» (далее по тексту Служба поддержки), предоставив достаточную информацию, как для первоначального анализа, так и для расширенного изучения причин нестабильного поведения.

Общая информация приведена в данном разделе ниже. Полные инструкции включаются в состав договоров на приобретение ПО или документации к договорам на приобретение ПО.

Обращение в Службу поддержки осуществляется через Сервер сопровождения.

Сервер сопровождения - программный ресурс, поддерживаемый ООО «СмартБанкинг» и доступный Клиенту посредством сети Интернет, при помощи которого ведётся регистрация заявок, официальная переписка и обмен необходимыми файлами в рамках установки и использования ПО согласно заключенным договорам. ООО «СмартБанкинг» в качестве Сервера сопровождения использует систему на базе Redmine, открытое серверное веб-приложение для управления проектами и задачами. Данные для доступа Клиенту к Серверу сопровождения предоставляются при подписании договоров о приобретении ПО.

Клиент может также обратиться по телефону +7(495)799-49-55.

При возникновении чрезвычайных ситуаций необходимо зарегистрировать обращение на Сервере сопровождения и обратиться к персональному менеджеру, контактные данные которого предоставляются при подписании договора о приобретении ПО.

Информация, необходимая для первоначального анализа ошибки ПО:

1. Краткое описание проблемной ситуации.
2. Полное описание проблемной ситуации, содержащее развернутую информацию:

о том, как и когда возникла данная неисправность, что ей предшествовало;

о том каким образом обнаружили и как она развивалась;

о том какие действия предпринимались персоналом для устранения причин возникновения.

3. Версия продукта.
4. Описание задействованных устройств, систем и протоколов их взаимодействия.
5. Скриншоты с сообщениями ПО.

По факту анализа представленной информации специалисты Службы поддержки вправе запросить дополнительную информацию.

При предоставлении информации, необходимой для первоначального анализа Ошибки ПО, рекомендуется:

Предоставлять скриншот с сообщением об ошибке максимально четкий и информативный.

"Снимок экрана" должен отражать как само сообщение об ошибке, так и место, в котором оно фиксируется.

Текст сообщения ПО рекомендуется сохранить и передать отдельным текстовым файлом.

"Чувствительные" персональные/корпоративные данные (пароли, контакты и т.п.), отраженные на скриншоте и в текстовом файле подробностей сообщения, необходимо скрывать (затемнять).