ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ЭЛЕКТРОННОЙ ПОДПИСИ БИОМЕТРИЧЕСКИХ ДАННЫХ ПРИ ПОДКЛЮЧЕНИИ К ЕДИНОЙ БИОМЕТРИЧЕСКОЙ СИСТЕМЕ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ ТИПОВОГО РЕШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Версия 1.12

Листов 121

Москва 2024

ИСТОРИЯ ДОКУМЕНТА

Версия	Дата	Автор	Комментарии
1.0	07.12.2018	Сеначин С.В.	Создание документа.
1.1	11.02.2019	Сеначин С.В.	Изменен раздел 2.2.4.1: тип выходного параметра функции.
1.2	12.02.2019	Сеначин С.В.	Изменен раздел 2.2.3.1: исправлено назначение функции
1.3	10.03.2019	Сеначин С.В.	Создан раздел 2.2.1
1.4	04.08.2020	Шишков А.А.	Отредактирован раздел 2.2.2
1.5	27.10.2021	Шляхова О.Ю.	Дополнен раздел 2.2.6
1.6	06.05.2022	Шляхова О.Ю.	Отредактирован раздел 2.2.6
1.7	02.11.2022	Копейкин С.Н.	Актуализирован раздел 2.2.6.1
1.8	03.11.2022	Копейкин С.Н.	1. Уточнены параметры базового URL в разделе 2.2.8 2. Уточнены параметры базового URL в разделе 2.2.9
1.9	29.09.2023	Гаврилов С.Р.	Изменено название документа, обновлены наименования ИС КА, КА, откорректированы определения, нормативные ссылки, добавлены процессы, разделы 2.2.4-2.2.7 сгруппированы в 2.2.4 (удаленная идентификация), добавлены разделы 2.2.7-2.2.14 из РП ТИБ, приложение 1 перенесено в п. 2.2.5, добавлены Приложение 1 (meta), Приложение 2 (metrics), Приложения 3-5, откорректированы и обновлены схемы, уточнены ГОСТы в п. 2.3, исправлены ошибки
1.10	16.11.2023	Гаврилов С.Р.	Изменена обязательность блока Matching в п. 4.12.1 и 4.13.2 и скорректировано описание
1.11	05.12.2023	Гаврилов С.Р.	Откорректированы тестовые запросы
1.12	27.03.2024	Липницкий И.В.	По всему тексту в документе были внесены изменения: - заменено доменное имя ebs-int.rtlabs.ru на int.ebs.ru

СОДЕРЖАНИЕ

СПИСОК ТЕРМИНОВ и СОКРАЩЕНИЙ 6
1 ВВЕДЕНИЕ 8
1.1 Назначение документа 8
1.2 Нормативные ссылки 8
1.3 Назначение 9
1.4 Характеристика объекта автоматизации 10
2 Общие требования и рекомендации 13
2.1 Требования к реализации процессов удаленной идентификации и регистрации БО 14
2.1.1 Требования к процессу удаленной идентификации 14
2.1.1.1 Требования к процессу удаленной идентификации пользователя в ЕБС с использованием мобильного устройства 16
2.1.1.2 Требования к процессу удаленной идентификации пользователя в ЕБС с использованием браузера 17
2.1.2 Требования к функциям процесса регистрации БО 19
2.2 Описание интерфейсов взаимодействий 20
2.2.1 Точка доступа к API 22
2.2.2 Поддерживаемые в запросах методы HTTP и типы контента 22
2.2.3 Используемые в API Адаптера коды ответов HTTP 24
2.2.4 API для организации процесса удаленной идентификации 25
2.2.4.1 Внутренний API верификации Адаптера с использованием ЕСИА 25
2.2.4.1.1 Функция "Создание сессии в Адаптере" 25
2.2.4.2 API верификации Адаптера, вызываемый пользовательскими устройствами 27
2.2.4.2.1 Функция "Запрос пользователя на начало аутентификации" 27
2.2.4.2.2 Функция "Получение доступа к биометрической верификации" 29
2.2.4.2.3 Функция "Передача результата верификации" 30
2.2.4.2.4 Функция "Получение параметра успешного завершения" 32
2.2.4.3 Спецификация API получения результата верификации ИС КА 33
2.2.4.3.1 Функция "Получение результата удаленной идентификации" 34
2.2.4.4 Спецификация API верификации ИС КА, вызываемого пользовательскими устройствами 39
2.2.4.4.1 Функция "Возврат пользователя в ИС КА" 39
2.2.5 Внутренний API Адаптера для биометрической регистрации (через СМЭВ) 40
2.2.5.1 Функция «Подписать сообщение для СМЭВ 3» 41
2.2.5.2 Функция «Проверить подпись» 45
2.2.6 Функция "Проверки состояния модулей Адаптера" 49
2.2.7 Внутренний API биометрической верификации с использованием IdP, отличного от ЕСИА 50

2.2.7.1 Функция «Создание сессии биометрической верификации» 50
2.2.7.2 Функция «Передача verify_token в Адаптер и возврат res_secret»....53
2.2.7.3 Функция «Передачи результатов биометрической верификации от Адаптера в ИС КА» 54
2.2.8 Внутренний API биометрической идентификации Адаптера 56
2.2.8.1 Функция "Создание сессии биометрической идентификации"....56
2.2.8.2 Функция «Передача verify_token в Адаптер и возврат res_secret»....59
2.2.8.3 Функция "Передачи результатов идентификации от Адаптера в ИС КА"....61
2.2.9 Внутренний API регистрации пользователя через API....62
2.2.9.1 Функция "Регистрация пользователя" 63
2.2.10 Внутренние API приостановки действия (деактивации) УЗ....70
2.2.10.1 Функция «Деактивация УЗ»....70
2.2.10.2 Функция «Деактивация БКШ» 72
2.2.11 Внутренний API удаления и получения БШ 74
2.2.11.1 Функция «Выгрузка БКШ»....74
2.2.11.2 Функция «Удаление БКШ»....77
2.2.12 Внутренние API информирования 78
2.2.12.1 Функция "Информирование ИС КА с функцией Поставщика БДн о результате регистрации УЗ " 78
2.2.12.2 Функция " Информирование ИС КА с функцией IdP о результате регистрации УЗ " 79
2.2.12.3 Функция "Информирование ИС КА с функцией IdP о результате связывания УЗ " 81
2.2.13 Внутренний API работы с согласиями в бумажном виде 82
2.2.13.1 Функция «Отправка согласия» 82
2.2.13.2 Функция «Отзыв согласия»....84
2.2.14 Внутренний API подписания и проверки подписи на ЕСИА-запросах....86
2.2.14.1 Функция «Подписание запроса на получение авторизационного кода ЕСИА» v1 86
2.2.14.2 Функция «Подписание запроса на получение авторизационного кода ЕСИА» v2 88
2.2.14.3 Функция «Подписание запроса на получение маркера доступа ЕСИА» v1 ...90
2.2.14.4 Функция «Подписание запроса на получение маркера доступа ЕСИА» v3 ...92
2.2.14.5 Функция «Проверки подписи на токенах, пришедших из ЕСИА» 95
2.3 Требования к поддерживаемым криптографическим алгоритмам 96
2.3.1 Требования к проверке ЭП в Адаптере....97
2.4 Требования к эксплуатации 97
2.5 Требования к численности, квалификации и функциям персонала Адаптера, режимам его работы 97
3 Требования к видам обеспечения....99

3.1 Требования к комплексу технических средств, его размещению на объекте.....99
3.1.1 Требования к размещению комплекса технических средств в инфраструктуре КА 99
3.1.2 Создание условий функционирования Адаптера 99
4 Требования к информационной безопасности.....100
4.1 Требования к техническим средствам защиты каналов взаимодействия.....100
4.2 Требования к защите информации от несанкционированного доступа 101
ПРИЛОЖЕНИЕ №1. Дополнительные метаданные (meta) 104
ПРИЛОЖЕНИЕ №2. Дополнительные данные о метриках системы (metrics).....108
ПРИЛОЖЕНИЕ №3. Виды метаданных поля BioMetadata (bio_metadata) 114
ПРИЛОЖЕНИЕ №4. Доступные мнемоники сбора БО в процессе биометрической верификации 115
ПРИЛОЖЕНИЕ №5. Доступные мнемоники сбора БО в процессе биометрической идентификации.....117

СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Наименование
АБС	Автоматизированная банковская система. В контексте данного документа состоит из системы дистанционного банковского обслуживания КА и ИС КА
Адаптер (Система)	Программно-аппаратный комплекс (ПАК) электронной подписи биометрических данных при подключении к Единой биометрической системе
БО	Биометрический образец
ДБО КО	Система дистанционного банковского обслуживания кредитной организации, термин используется в контексте процесса удаленной идентификации
ИС КА	Информационная система контрагента, осуществляющая сбор и отправку в ЕБС биометрических образцов клиента (регистрация биометрических образцов)
ЕБС	Единая биометрическая система
ЕСИА	Единая система идентификации и аутентификации
КА	Контрагент - организации, осуществляющие аутентификацию на основе биометрических персональных данных физических лиц с использованием ЕБС, названные в части 1 статьи 10 и части 1 статьи 16 Федерального закона от 29.12.2022 № 572-ФЗ, в том числе кредитные организации, некредитные финансовые организации, субъекты национальной платежной системы, лица, оказывающие профессиональные услуги на финансовом рынке (страховые организации, биржевые брокеры и т.д.), иные организации (вне зависимости от формы собственности организации – ООО, АО и т.д.), индивидуальные предприниматели, нотариусы.
Контролируемая зона КА	Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) КА и лиц, не имеющих постоянного допуска на объекты ИС КА (не являющихся работниками КА), а также транспортных, технических и иных материальных средств. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите персональных данных и в соответствии с требованиями к эксплуатации СКЗИ, входящих в состав ПАК.
МП	Мобильное приложение
МП Госуслуги Биометрия	Мобильное приложение Госуслуги Биометрия для взаимодействия с Единой биометрической системой
МП КА	Мобильное приложение контрагента
Пользователь ЕБС	Физическое лицо (гражданин Российской Федерации), взаимодействующее с Единой биометрической системой с целью получения услуг с использованием биометрических сервисов Единой биометрической системы
ПДн	Персональные данные
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
СМЭВ	Система межведомственного электронного взаимодействия

Сокращение	Наименование
СОС	Список отозванных сертификатов
СПО	Специальное программное обеспечение автоматизированной системы. Часть программного обеспечения, представляющая собой совокупность программ, разработанных при создании данной автоматизированной системы.
ТИБ	Типовое решение информационной безопасности ПАК электронной подписи биометрических данных при подключении к Единой биометрической системе
ТК 26	Технический комитет по стандартизации «Криптографическая защита информации»
ФЛ	Физическое лицо
ФСБ России	Федеральная служба безопасности России
ФСТЭК России	Федеральная служба по техническому и экспортному контролю России
ЭП	Электронная подпись
API	Application Programming Interface (прикладной программный интерфейс)
ECC	Error-Correcting Code memory (память с коррекцией ошибок)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	HyperText Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования в целях повышения безопасности)
HSM	Hardware Security Module (программно-аппаратный криптографический модуль)
JWT	JSON Web Token (JSON объект, который определен в открытом стандарте RFC 7519)
OCSP	Online Certificate Status Protocol (протокол проверки статуса сертификата)
SNMP	Simple Network Management Protocol (простой протокол сетевого управления)
SOAP	Simple Object Access Protocol (простой протокол доступа к объектам)
TLS	Transport Layer Security (протокол безопасной передачи данных)

1 ВВЕДЕНИЕ

1.1 Назначение документа

Требования, указанные в документе, следует рассматривать в дополнение к требованиям, содержащимся в нормативно-правовых документах, регламентирующих работу Единой Биометрической Системы (далее ЕБС).

В рамках документа рассматриваются следующие вопросы:

- Процесс удаленной идентификации с использованием ЕСИА и ЕБС;
- Процесс биометрической верификации;
- Процесс биометрической идентификации;
- Процесс связывания учетных записей;
- Процесс регистрации биометрических данных в ЕБС;
- Процесс импорта БО и предоставления (выгрузки) векторов (БШ);
- Процесс удаления БКШ;
- Процесс деактивации БО;
- Процесс передачи информации о согласии Пользователя, полученном (или отозванном) в бумажном виде;
- Процесс подписания и проверки подписи запросов необходимых для взаимодействия с ЕСИА.

Документ содержит требования и рекомендации по использованию программно-аппаратного комплекса электронной подписи биометрических данных при подключении к Единой Биометрической Системе.

Описываемые в документе правила являются обязательными к применению участниками биометрического взаимодействия ЕБС, в том числе с использованием Системы межведомственного электронного взаимодействия (СМЭВ 3.x) и Единой системы идентификации и аутентификации (ЕСИА).

1.2 Нормативные ссылки

Законодательные, нормативно-правовые и иные акты и документы:

1. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – Федеральный закон №572-ФЗ);
2. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее - Федеральный закон №63-ФЗ);
3. Федеральный закон РФ от 27.07.2006 №152-ФЗ «О персональных данных» (далее -

Федеральный закон №152-ФЗ);

4. Федеральный закон РФ от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ);
5. Указание Банка России от 16.12.2021 №6017-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой» (далее – Указание №6017-У);
6. Методические рекомендации по работе с ЕБС для разработчиков (размещаются по адресу https://ebs.ru/documents/ в разделе «Основные»);
7. Методические рекомендации по использованию сервисов выгрузки векторов и импорту БО (размещаются по адресу https://ebs.ru/documents/ в разделе «Основные»);
8. Методические рекомендации по использованию сервиса биометрической верификации (размещаются по адресу https://ebs.ru/documents/ в разделе «Основные»);
9. Руководство пользователя по работе с библиотекой ЕБС.SDK (размещается по адресу https://ebs.ru/documents/ в разделе «Софт»);
10. Методические рекомендации по работе с СМЭВ 3.x (размещаются по адресу https://smev3.gosuslugi.ru/portal/ в разделе «Технологические стандарты и рекомендации»);
11. Методические рекомендации по использованию ЕСИА (последняя версия размещается по адресу https://digital.gov.ru/documents/6186/);
12. Регламенты и инструкции для подключения к СМЭВ 3.x (размещаются по адресу https://info.gosuslugi.ru/docs/ в разделе «СМЭВ 3»);
13. Регламент информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства (последняя версия размещается по адресу https://digital.gov.ru/ru/documents/4244/);

1.3 Назначение

Назначением программно-аппаратного комплекса электронной подписи биометрических данных при подключении к Единой Биометрической Системе (далее Адаптер) является обеспечение возможности для организаций проведения удаленной электронной биометрической идентификации Пользователей ЕБС по биометрическим характеристикам (удаленная идентификация), биометрической верификации с привязкой к идентификаторам учетных записей различных Провайдеров идентификации, размещения или обновления в ЕБС БПДн (регистрация БО), проведения импорта БО, выгрузки БШ, удаления БШ, деактивации БО, работы с согласиями пользователя в бумажном виде, подписания и проверки подписи на запросах ЕСИА для исполнения требований, установленных Федеральным законом № 115-ФЗ, Федеральным законом № 572-ФЗ и

размещения или обновления в Единой биометрической системе биометрических персональных данных.

1.4 Характеристика объекта автоматизации

Согласно Федеральному закону №115-ФЗ, КА – кредитные организации вправе открывать и вести счета (вклады) клиентов - физических лиц, предоставлять кредиты клиентам - физическим лицам, а также осуществлять переводы денежных средств по таким счетам по их поручению без их личного присутствия после проведения идентификации клиентов - физических лиц путем установления и подтверждения достоверности сведений о них, определенных настоящим Федеральным законом, с использованием единой системы идентификации и аутентификации и единой биометрической системы (далее – удаленная идентификация);

КА обязан после проведения идентификации при личном присутствии клиента - физического лица, являющегося гражданином РФ, с его согласия и на безвозмездной основе размещать или обновлять в Единой биометрической системе его биометрические персональные данные (далее – регистрация БО).

Для реализации этих прав и обязанностей КА необходимо:

- выполнить интеграцию с ЕСИА в части аутентификации ФЛ по протоколам OAuth и OpenId Connect в соответствии с Методическими рекомендациями по использованию Единой системы идентификации и аутентификации – для проведения удаленной идентификации с использованием ЕСИА и ЕБС;
- выполнить интеграцию с ЕБС в соответствии с Методическими рекомендациями по работе с Единой биометрической системой – для проведения удаленной идентификации с использованием ЕСИА и ЕБС;
- выполнить интеграцию со СМЭВ 3 в соответствии с Методическими рекомендациям по работе с Единой системой межведомственного электронного взаимодействия (СМЭВ 3.xx) – для размещения или обновления в ЕБС биометрических персональных данных.

При проведении удаленной идентификации с использованием ЕБС посредством сети "Интернет" должны применяться шифровальные (криптографические) средства.

В случае, если физическое лицо для удаленной идентификации с использованием ЕБС использует мобильный телефон, смартфон или планшетный компьютер и отказывается от использования шифровальных (криптографических) средств, необходимо отказать такому лицу в проведении указанной идентификации.

Адаптер к ЕСИА и ЕБС реализует необходимые протоколы обмена с ЕСИА и ЕБС, обеспечивает формирование и проверку ЭП, что упрощает для КА реализацию бизнес-процессов регистрации БО и удаленной идентификации с использованием ЕБС.

Адаптер обеспечивает:

- интеграцию с ЕСИА для аутентификации пользователя с последующим получением ПДн;
- интеграцию с ЕБС для проведения биометрической верификации в рамках процесса удаленной идентификации по требованиям Федерального закона №115-ФЗ с использованием ЕБС;
- интеграцию с ЕБС для проведения биометрической верификации вне процесса удаленной идентификации (вне требований Федерального закона №115-ФЗ) с использованием Провайдера идентификации, отличного от ЕСИА;
- интеграцию с ЕБС для передачи персональных биометрических данных в ЕБС (проведения импорта);
- интеграцию с ЕБС для проведения биометрической идентификации пользователей по предоставленным биометрическим образцам (по схеме «один ко многим») среди биометрических данных, хранящихся в ЕБС;
- формирование пакетов данных СМЭВ для передачи БО в ЕБС;
- интеграцию с ЕБС для получения БШ, созданных в ЕБС в процессах биометрической регистрации и импорта БО;
- интеграцию с HSM разных производителей, в том числе ПАКМ «КриптоПро HSM» версии 2.0, для безопасного хранения и использования секретных ключей электронной подписи (отечественные криптографические алгоритмы);
- поддержку западных и отечественных криптографических алгоритмов в части взаимодействия по протоколу TLS;
- простой API для интеграции с ИС КА.

Адаптер позволяет КА реализовать требования по информационной безопасности в части обеспечения целостности, конфиденциальности, достоверности биометрических данных при обработке, включая сбор и хранение, их передаче в ЕБС, получении информации о степени соответствия предъявленных биометрических данных.

Для решения задач Адаптер выполняет следующие группы (комплексы) внутренних функций:

- группа функций процесса верификации для решения задачи работы в рамках протокола OpenId Connect со стороны клиента (КА, проводящего авторизацию пользователя с использованием его биометрических данных - удаленную идентификацию) (внутренний API верификации Адаптера);
- группа функций процесса аутентификации (внутренние API);
- группа функций получения результата верификации для ИС КА (API получения результата верификации ИС КА);
- группа функций процесса регистрации БО для решения задачи формирования и

проверки электронной подписи передаваемых в ЕБС собираемых биометрических данных (внутренний API регистрации Адаптера);

- группа функций проверки электронной подписи передаваемых в ЕБС собираемых биометрических данных (внутренний API подписания Адаптера);
- группа функций процесса регистрации УЗ Пользователя в ГИС ЕБС (внутренние API);
- группа функций процесса выгрузки БШ для ИС КА (внутренние API);
- группа функций процесса удаления БШ в ИС КА (внутренние API);
- группа функций процесса информирования для ИС КА (внутренние API);
- группа функций процесса деактивации УЗ в ГИС ЕБС (внутренние API);
- группа функций процесса деактивации БКШ в ГИС ЕБС (внутренние API);
- группа функций процесса передачи информации о согласиях (внутренние API);
- группа функций процесса подписания запроса в ЕСИА (внутренние API);
- группа функций процесса проверки подписи на токенах ЕСИА (внутренние API).

2 ОБЩИЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

Структурная схема взаимодействия Адаптера и смежных систем в контексте процессов, указанных в п. 1.4, с указанием требований к защите каналов взаимодействия приведена на рисунке ниже (см. **Ошибка! Источник ссылки не найден.**)

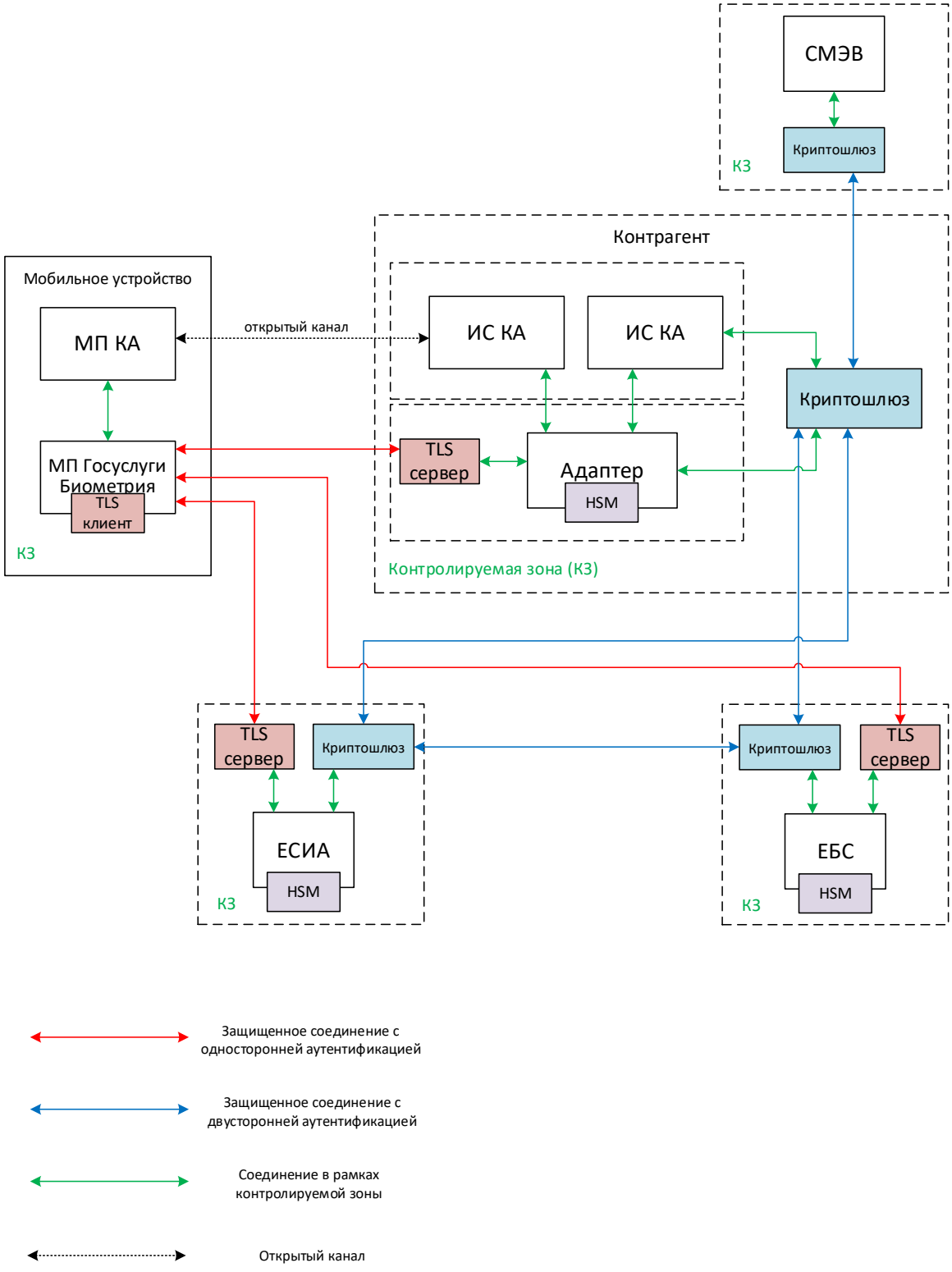


Рисунок 1 Структурная схема взаимодействия Адаптера

2.1 Требования к реализации процессов удаленной идентификации и регистрации БО

2.1.1 Требования к процессу удаленной идентификации

Протокол процесса удаленной идентификации подразумевает взаимодействие между следующими участниками:

- ЕСИА;
- ЕБС;
- КА, состоящий из ИС КА и Адаптера;
- Пользователь, зарегистрированный в ЕСИА и ЕБС (далее – пользователь).

Пользователь может взаимодействовать с КА двумя способами:

- с помощью браузера;
- с помощью МП КА и МП Госуслуги Биометрия.

Данный протокол предназначен для проведения идентификации и аутентификации пользователя, запрашивающего доступ к ресурсам КА. После успешного выполнения протокола пользователь и ИС КА находятся в следующем состоянии:

- у пользователя (в МП КА или браузере) появляется параметр успешного завершения протокола "res_secret" (см. Рисунок 2), который пользователь передает в ИС КА, позволяя КА аутентифицированным образом провести запрашиваемую пользователем бизнес-операцию;
- у ИС КА появляется параметр успешного завершения протокола "res_secret", совпадающий с тем, который есть у пользователя. С данным значением у ИС КА связан расширенный результат биометрической верификации и персональные данные пользователя.

По завершении протокола удаленной идентификации пользователь предъявляет ИС КА параметр успешного завершения протокола "res_secret" (далее - параметр "res_secret") для выполнения бизнес-операции в КА аутентифицированным образом.

Требования к использованию параметра "res_secret" в ИС КА:

- параметр "res_secret" должен использоваться для выполнения только одной бизнес-операции в ИС КА;
- срок жизни параметра "res_secret" в ИС КА должен составлять не более 15 минут. По истечении данного интервала времени параметр res_secret должен объявляться в ИС КА невалидным, связанные с ним сессионные параметры должны удаляться.

На рисунке ниже (Рисунок 2) представлена высокоуровневая схема взаимодействия участников протокола удаленной идентификации с использованием ЕБС.

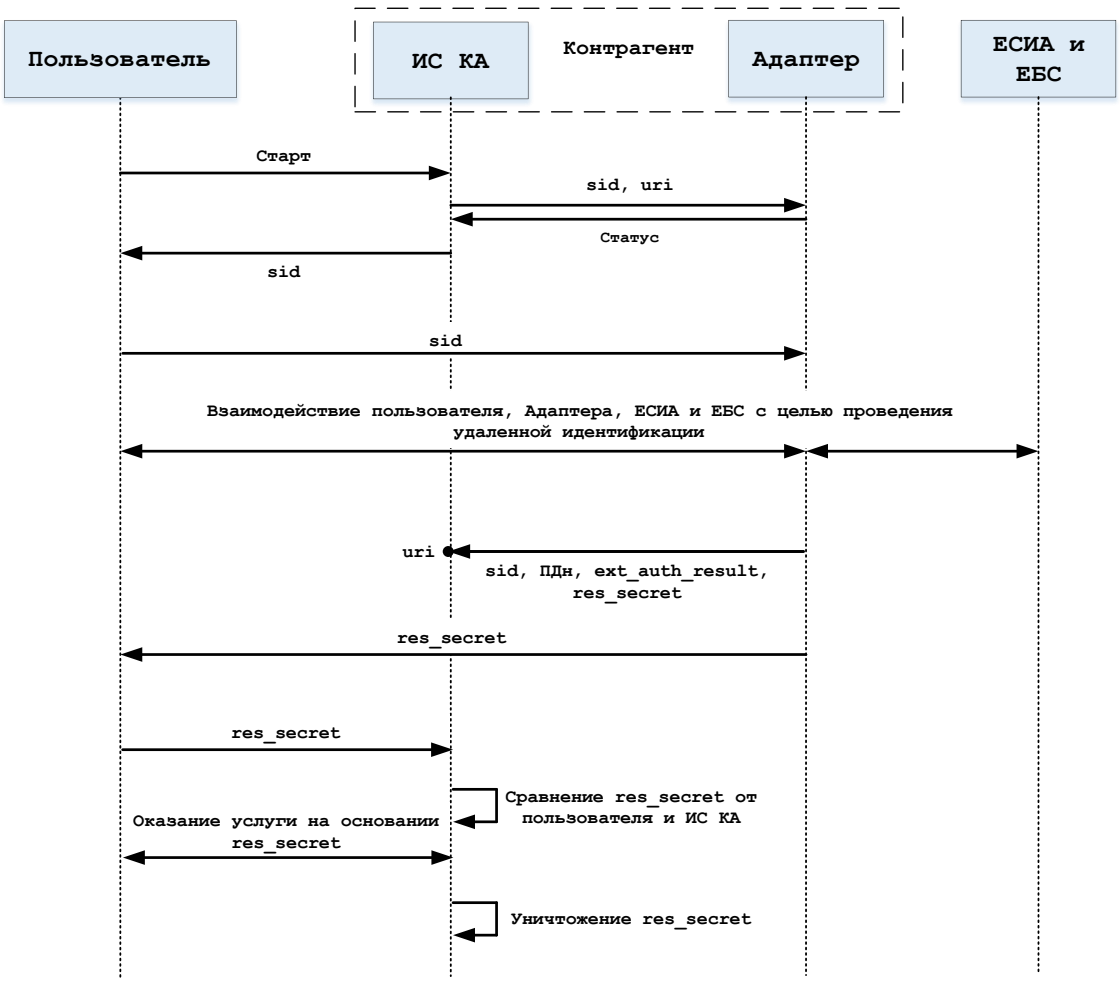


Рисунок 2 Схема взаимодействия участников протокола удаленной идентификации с использованием ЕБС

Обозначения, принятые на схеме (см. Рисунок 2):

- sid: сгенерированный ИС КА идентификатор сессии;
- uri: URL "API получения результата верификации ИС КА", на который Адаптер должен вернуть результат биометрической верификации и ПДн пользователя;
- ext_auth_result: расширенный результат биометрической верификации;
- res_secret: параметр, который пользователь предъявляет ИС КА по завершении протокола удаленной идентификации для выполнения бизнес-операции в КА аутентифицированным образом.

На рисунках ниже представлены детальные схемы взаимодействия участников протокола удаленной идентификации с использованием МП и браузера. В случае использования браузера взаимодействие осуществляется аналогичным образом, как и при использовании МП. При этом необходимо, чтобы на стороне пользователя было установлено ПО, реализующее взаимодействие в браузере по протоколу TLS с использованием отечественных криптографических алгоритмов, для обеспечения защищенного взаимодействия. В качестве такого решения допустимо использовать

СКЗИ с браузерами Internet Explorer, Спутник, Яндекс Браузер, при условии соответствия данных продуктов требованиям по информационной безопасности ФСБ России.

2.1.1.1 Требования к процессу удаленной идентификации пользователя в ЕБС с использованием мобильного устройства

Требования к реализации процесса удаленной идентификации пользователя в ЕБС с использованием мобильного устройства приведены на схеме ниже (см. **Ошибка! Источник ссылки не найден.**).

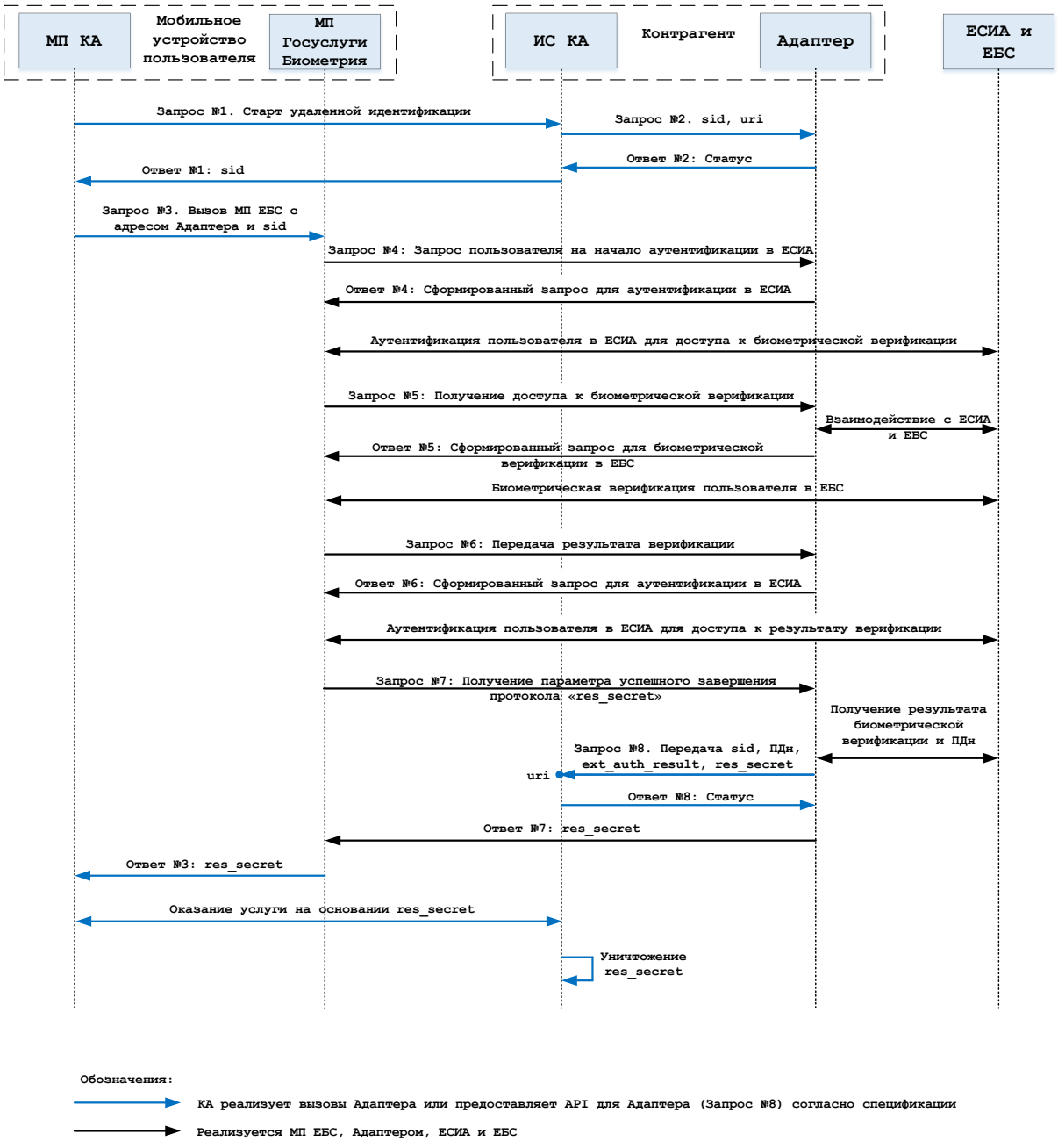


Рисунок 3 Процесс удаленной идентификации пользователя в ЕБС с использованием мобильного устройства

Описание интерфейсов взаимодействия для запросов и ответов, которые реализует КА, приведено в разделе 2.2 настоящего документа, за исключением запроса и ответа вызова мобильного приложения ЕБС: запрос и ответ №3 на схемах **Ошибка! Источник ссылки не найден.**. Описание данного взаимодействия (запрос и ответ №3) реализуется согласно Методическим рекомендациям по работе с ЕБС.

Запрос и обработку ответа №8 на диаграмме взаимодействия выполняет Адаптер. ИС КА должна предоставить для Адаптера данный API (см. п. 2.2.4.3.1).

2.1.1.2 Требования к процессу удаленной идентификации пользователя в ЕБС с использованием браузера

Требования к реализации процесса удаленной идентификации пользователя в ЕБС с использованием браузера приведены на схеме ниже (см. **Ошибка! Источник ссылки не найден.**).

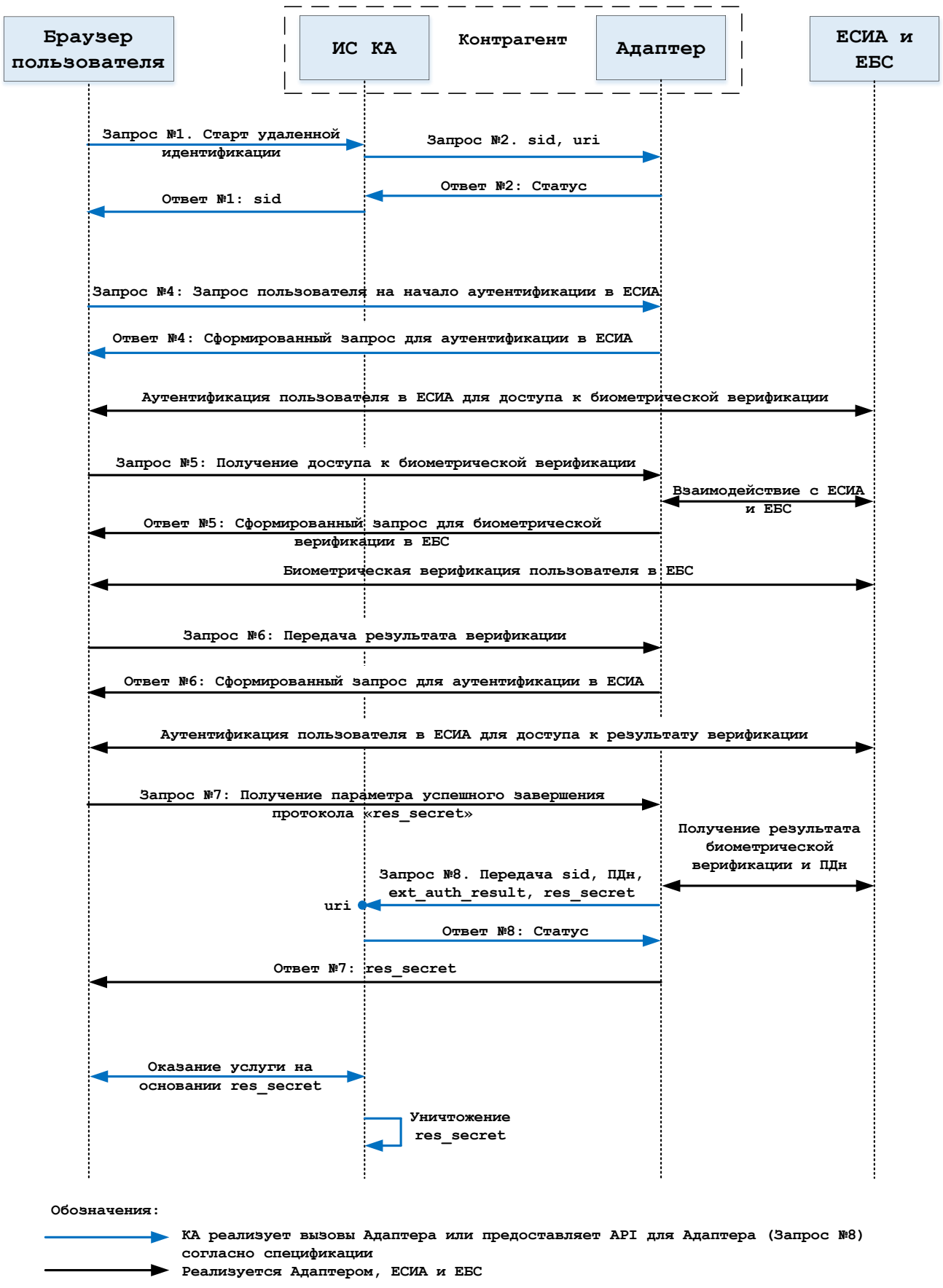


Рисунок 4 Процесс удаленной идентификации пользователя в ЕБС с использованием браузера

Описание интерфейсов взаимодействия для запросов и ответов, которые реализует КА, приведено в разделе **Ошибка! Источник ссылки не найден.** настоящего документа. Запрос и обработку ответа №8 на диаграмме взаимодействия выполняет Адаптер. ИС КА должна предоставить для Адаптера данный API (см. п. 2.2.4.3.1).

2.1.2 Требования к функциям процесса регистрации БО

Процесс регистрации БО подразумевает взаимодействие между следующими участниками:

- ЕСИА;
- ЕБС;
- СМЭВ 3;
- ИС КА и Адаптера на стороне КА.

Для получения возможности прохождения удалённой идентификации через ИС КА (см. раздел **Ошибка! Источник ссылки не найден.**) физическое лицо должно лично обратиться в КА с целью прохождения процедуры биометрической регистрации.

Снятие БО производит сотрудник КА (оператор регистрации БО) при помощи ИС КА. Биометрические образцы клиента проверяются в ИС КА с помощью, поставляемой ЕБС библиотеки контроля качества на соответствие требованиям, после чего данные БО с дополнительной информацией передаются в ЕБС.

Передача БО от КА в ЕБС должна осуществляться с использованием Единой системы межведомственного информационного взаимодействия (СМЭВ 3) в соответствии с действующими методическими рекомендациями СМЭВ 3.

Передаваемые БО клиента должны быть связаны с уникальным идентификатором клиента в ЕСИА. Для выполнения этого требования оператор регистрации БО должен осуществить поиск учетной записи (далее УЗ) клиента в ЕСИА до передачи БО от КА в ЕБС. При отсутствии УЗ ЕСИА, оператор регистрации БО должен осуществить регистрацию УЗ клиента в ЕСИА. Поиск и регистрацию УЗ клиента в ЕСИА оператор регистрации БО осуществляет при помощи ИС КА.

Взаимодействие ИС КА с ЕСИА для поиска и регистрации УЗ клиента должно осуществляться с использованием Единой системы межведомственного информационного взаимодействия (СМЭВ 3) в соответствии с действующими методическими рекомендациями СМЭВ 3 и в соответствии с действующими методическими рекомендациями (в части использования ВС ЕСИА).

На рисунке ниже (см. **Ошибка! Источник ссылки не найден.**) представлена высокоуровневая схема взаимодействия участников процесса регистрации БО. После успешного выполнения процесса биометрические образцы клиента КА будут успешно зарегистрированы в ЕБС.

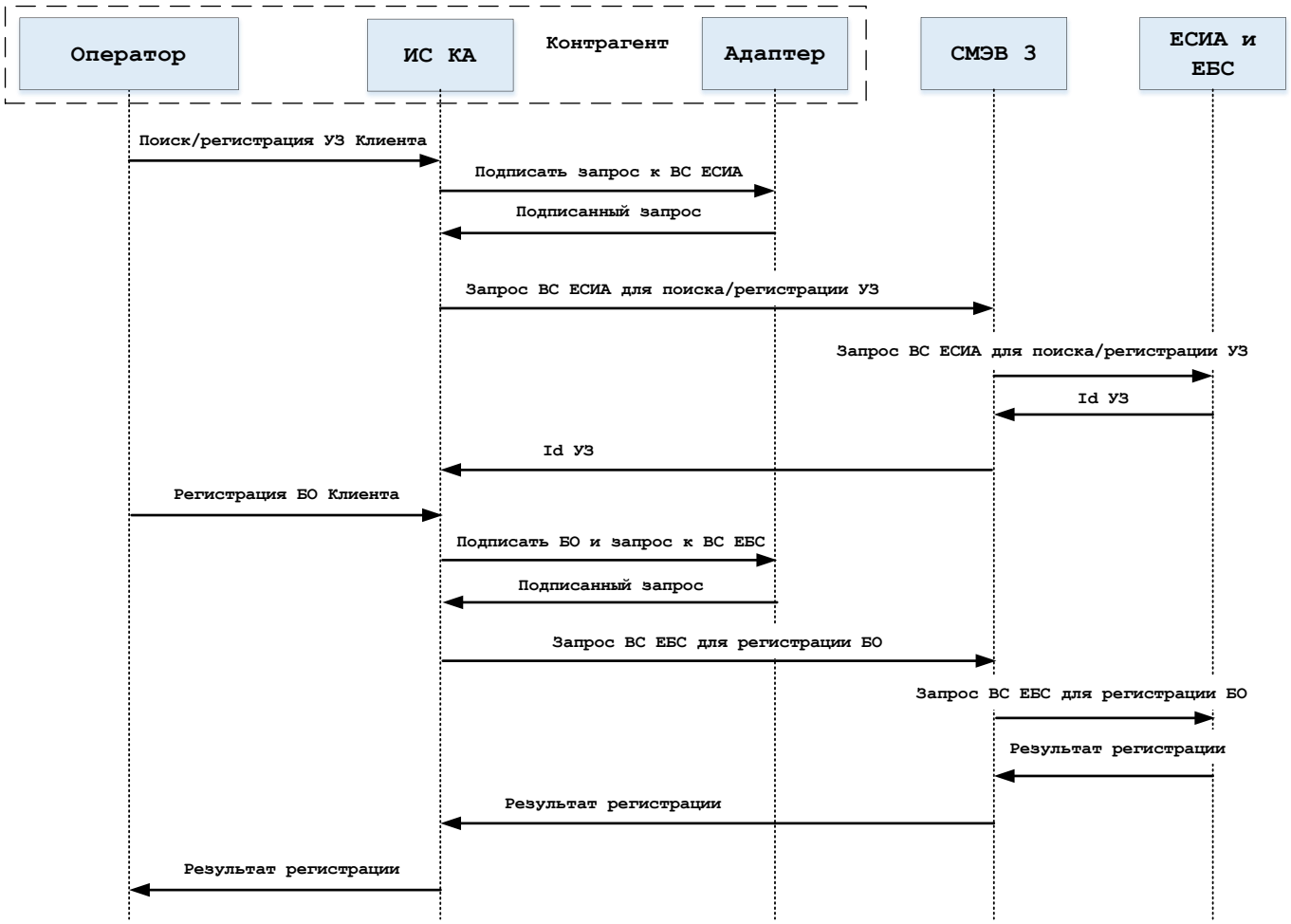


Рисунок 5 Процесс взаимодействия участников процесса регистрации БО

В электронных сообщениях, передаваемых через СМЭВ, применяются усиленные квалифицированные электронные подписи. Участник взаимодействия - КА, являющийся в данном контексте "потребителем" видов сведений ЕСИА и ЕБС, должен осуществлять:

- подписывать ЭП запросы к ВС ЕСИА и ЕБС при отправке их в СМЭВ 3;
- проверять ЭП ответов СМЭВ 3 на отправленные запросы к ВС ЕСИА и ЕБС.

Данные функции для ИС КА осуществляет Адаптер: ИС КА вызывает API регистрации Адаптера для формирования или проверки ЭП (см. п. 2.2.5).

2.2 Описание интерфейсов взаимодействий

Требования к схеме взаимодействий со смежными системами и используемых при обмене API в рамках процессов удаленной идентификации и регистрации БО приведена на рисунке **Ошибка! Источник ссылки не найден.** (**Ошибка! Источник ссылки не найден.**).

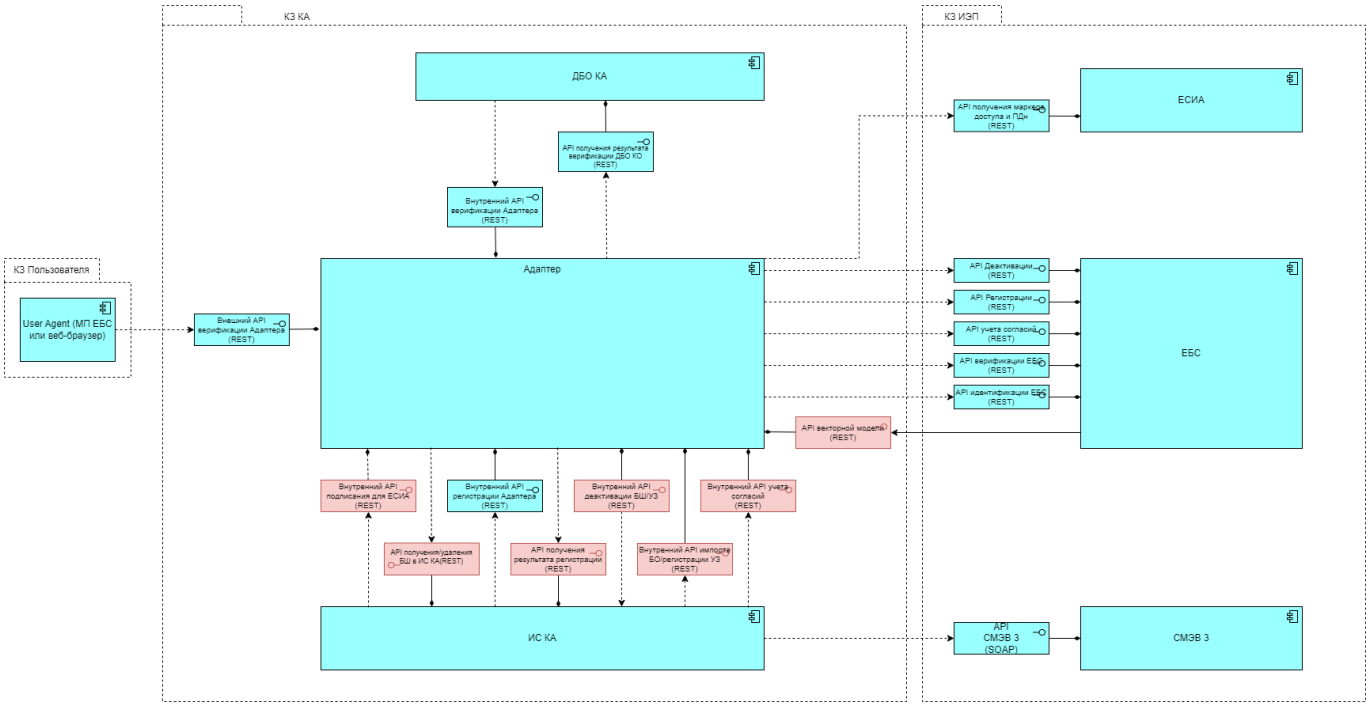


Рисунок 6 Схема взаимодействия со смежными системами и используемых при обмене API в рамках процессов удаленной идентификации и регистрации БО

Взаимодействие Адаптера со смежными системами осуществляется с использованием следующих API:

- API для взаимодействия с Адаптером в рамках протокола удаленной идентификации (п. 2.2.4):
  - Внутренний API верификации Адаптера. Доступен для вызовов только из ИС КА в пределах контролируемой зоны КА. Описание API приведено в п 2.2.4.1;
  - API верификации Адаптера, вызываемый пользовательскими устройствами. Доступен для вызовов из сети Интернет. Описание API приведено в разделе 2.2.4.2;
  - API получения результата верификации ИС КА. Доступен для вызовов только из Адаптера в пределах контролируемой зоны КА. Описание API приведено в п. 2.2.4.3;
  - API верификации ИС КА, вызываемый пользовательскими устройствами. Доступен для вызовов из сети Интернет. Описание API приведено в п. 2.2.4.2.
- Внутренний API Адаптера для биометрической регистрации (через СМЭВ). Доступен для вызовов только из ИС КА в пределах контролируемой зоны КА. Описание API приведено в п. 2.2.5;
- Внутренний API биометрической верификации Адаптера с использованием Провайдера идентификации, отличного от ЕСИА. Описание API приведено в п.

2.2.7;

- Внутренний API биометрической идентификации Адаптера. Описание API приведено в п. 2.2.8;
- Внутренний API регистрации пользователя. Описание API приведено в п. 2.2.9;
- Внутренний API приостановки действия (деактивации) УЗ. Описание API приведено в п. 2.2.10;
- Внутренний API удаления и получения БКШ. Описание API приведено в п. 2.2.11;
- Внутренний API информирования ИС КА о результате регистрации и связывании УЗ. Описание API приведено в разделе 2.2.12;
- Внутренний API работы с согласиями в бумажном виде. Описание API приведено в разделе 2.2.13;
- Внутренний API подписания и проверки подписи на ЕСИА-запросах. Описание API приведено в разделе 2.2.14.

Информационный обмен Адаптера с ЕСИА реализован в соответствии с Методическими рекомендациям по использованию Единой системы идентификации и аутентификации.

Информационный обмен Адаптера с ЕБС реализован в соответствии с Методическими рекомендациями по работе с Единой биометрической системой.

2.2.1 Точка доступа к API

Базовый URL доступа к API Адаптера:

```
https://{{adapter_url}}/api/v{{version}},
```

где {{adapter_url}} - имя хоста и (опционально) порт API Адаптера,

{{version}} - номер версии API.

Актуальные версии API: «v1», «v2».

Формат версии: префикс «v» и целое число.

2.2.2 Поддерживаемые в запросах методы HTTP и типы контента

Система поддерживает следующие методы HTTP:

- GET
- POST

Адаптер поддерживает следующие типы контента запроса (HTTP-заголовок «Content-Type»):

В процессе регистрации:

- «application/xml»;
- «application/json»;
- «multipart/form-data».

В процессе удаленной идентификации (по Федеральному закону №115-ФЗ):

- «application/xml»;
- «application/json»;

В процессе биометрической верификации (не ЕСИА):

- «application/json»;

В процессе биометрической идентификации:

- «application/json»;

В процессе импорта БО/регистрации УЗ:

- «application/json»;
- «multipart/form-data».

Входные параметры метода передаются в виде строки запроса[1] (часть URL после знака «?», разделитель параметров — знак «&») с передаваемыми на сервер параметрами при использовании метода GET, либо в теле POST-запроса. В случае GET-запроса параметры должны быть закодированы с помощью URL Encoding[2], т.к. для URL доступны только символы латинского алфавита. При наличии тела запроса (метод POST), его содержимое (входные параметры метода) должно быть передано в формате JSON[3].

Если тип контента POST-запроса - «application/json», то входные параметры метода передаются в теле POST-запроса в формате JSON.

Если тип контента POST-запроса - «multipart/form-data», то данные (отдельно каждый БО и отдельно остальные данные) передается как отдельная часть составного содержимого HTTP-запроса и следует правилам для составных MIME-данных в соответствии с RFC 2045.

Каждая часть должна содержать:

- заголовочное поле «Content-Disposition», имеющее значение «form-data»;
- атрибут «name» поля «Content-Disposition», имеющий значение, равное наименованию входного параметра (см. ниже таблицы с описанием входных параметров соответствующих методов);
- атрибут «filename» поля «Content-Disposition», принимающий значение имени файла;
- заголовочное поле «Content-Type», принимающее значение в зависимости от контента, передаваемого в части:
  - входные параметры функции (см. раздел 2.2.5.1): «application/xml»;
  - биометрический образец: в зависимости от MIME типа вложения - биометрического образца, регистрируемого в ЕБС (см. раздел 2.2.5.1).

1 Согласно RFC 3984, раздел 3.4
2 Согласно RFC 3986, раздел 2.1
3 Согласно RFC 7159

Следует отметить, что boundary (граница) — это последовательность байтов, которая не должна встречаться внутри закодированного представления данных части.

В каждом HTTP-запросе присутствует набор обязательных параметров, но могут быть определены дополнительные параметры, требуемые только для конкретного метода. Текстовые значения параметров передаются в кодировке UTF-8.

2.2.3 Используемые в API Адаптера коды ответов HTTP

Предоставляемые Адаптером смежным системам API используют коды ответов HTTP, которые приведены в таблице ниже.

Код ответа	Примечания
200 OK	Вызов метода завершился успешно. Ответ Сервера включен в HTTP BODY.
302 Found	Вызов метода завершился успешно, требуется перенаправление пользователя.
400 Bad Request	Вызов метода завершился с ошибкой на стороне клиента (вызывающей системы). Код ошибки включен в HTTP BODY.
401 Unauthorized	Вызов метода завершился с ошибкой: запрос защищенного ресурса без предоставления необходимых данных авторизации (отсутствует маркер доступа, ошибка проверки маркера доступа и т.п.)
500 Internal Server Error	Вызов метода завершился с ошибкой на стороне сервера (ЕБС). Код ошибки включен в HTTP BODY.

Интерфейсы, их схема взаимодействия и коды возврата могут уточняться на этапе разработки и проведения исследований, предусмотренных настоящим документом.

Все успешные ответы, не требующие перенаправления пользователя:

- содержат код ответа HTTP 200;
- возвращают JSON объект со значениями выходных параметров метода в HTTP BODY, в случае наличия выходных параметров в ответе. Тип контента - «application/json».

Все успешные ответы, требующие перенаправления пользователя:

- в заголовке Location указан URL, на который необходимо перенаправить пользователя.

Все синхронные ответы с ошибкой смежным системам (ИС КА, КА):

- содержат код ответа HTTP 40x или 500;
- возвращают JSON объект с описанием ошибки в HTTP BODY. Тип контента «application/json».

Примечание: в отдельных случаях (фатальная ошибка на стороне Адаптера) ответы с кодом HTTP 500 могут не содержать HTTP BODY.

Пример ответа с ошибкой:

```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8
```

```
{
  "code": "ADR-0003",
  "message": "Недействительный токен доступа"
}
```

В случае возникновения ошибки в процессе выполнения протокола удаленной идентификации (внутренние ошибки Адаптера, ошибки взаимодействия с ЕСИА и ЕБС, ошибки обработки запросов пользователя к внешнему API верификации) Адаптер:

- передает в ИС КА код ошибки и ее описание (см. п. 2.2.4.3.1);
- перенаправляет пользователя на внешний API верификации ИС КА (доступный из сети Интернет URL ИС КА) (см. п. 2.2.4.4.1).

2.2.4 API для организации процесса удаленной идентификации

2.2.4.1 Внутренний API верификации Адаптера с использованием ЕСИА

Используется ИС КА для старта процесса аутентификации с использованием IDP ЕСИА и ЕБС. Вызовы осуществляются в пределах контролируемой зоны КА.

Реализация:

Аспект реализации	Реализация
Транспортный протокол	HTTPS
Аутентификация вызывающей стороны	Authorization - обязательный заголовок в запросе. Имеет вид Authorization: Bearer токен_доступа. Токен доступа прописывается в конфигурации Адаптера и выдается ППО ИС КА.

2.2.4.1.1 Функция "Создание сессии в Адаптере"

Запрос №2 на диаграмме взаимодействия

Вызывается ИС КА (ДБО КО) для старта процесса удаленной идентификации с использованием ЕСИА и ЕБС. Результатом является создание контекста сессии в Адаптере, идентифицируемой по полученному от ИС КА идентификатору.

Поддерживаемый метод HTTP запроса:

```
POST
```

Путь, относительно базового URL:

```
/vrf/create
```

Заголовки запроса:

```
Authorization: Bearer {{token}}
Content-Type: application/json,
```

где {{token}} - токен доступа ИС КА к API.

Входные параметры в теле запроса в формате JSON:

Параметр	Тип данных	Обязательность	Описание
sid	UUID	Да	Идентификатор сессии.
dbo_ko_uri	Строка	Да	URL "API получения результата верификации ИС КА" (ДБО КО), на который Адаптер должен вернуть результат биометрической верификации и ПДн пользователя
dbo_ko_public_uri	Строка	Да	Публичный (доступный из сети Интернет) URL ИС КА (ДБО КО), на который Адаптер должен перенаправить пользователя в случае успешного завершения процесса удаленной идентификации или возникновения ошибки.

Успешный ответ: выходные параметры отсутствуют.

Пример запроса:

```
POST /api/v1/vrf/create HTTP/1.1
Authorization: Bearer FAEA055D4EE948CEA031ACE10ECDAE49
Content-Type: application/json

{
  "sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
  "dbo_ko_uri": "https://192.168.0.2/path",
  "dbo_ko_public_uri": "https://dbo.test.bank.ru/public-path"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
```

Прикладные ошибки:

Код ответа HTTP	Значение параметра «code»	Описание (параметр «message»)
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа
400	ADR-0200	Сессия уже существует
400	ADR-0203	Невалидный Authorization Bearer
500	ADR-0205	Внутренняя ошибка при работе с базой данных
500	ADR-0206	Попытка перехода сессии пользователя в запрещенное состояние

2.2.4.2 API верификации Адаптера, вызываемый пользовательскими устройствами

Не реализуется ИС КА, используется пользователем (браузер или мобильное приложение) для аутентификации с использованием ЕСИА и ЕБС.

Взаимодействие осуществляется по защищенному каналу (HTTPS с российскими или, опционально, зарубежными (см. раздел **Ошибка! Источник ссылки не найден.**) криптографическими алгоритмами. HTTPS терминируется на TLS-шлюзе Адаптера.

Реализация:

Аспект реализации	Реализация
Транспортный протокол	(HTTPS с российскими криптографическими алгоритмами, односторонняя аутентификация сервера)

2.2.4.2.1 Функция "Запрос пользователя на начало аутентификации"

Запрос №4 на диаграммах взаимодействия (см. п. **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Вызывается пользователем для старта процесса аутентификации с использованием ЕСИА и ЕБС. Результатом является перенаправление на ЕСИА для аутентификации пользователя.

Поддерживаемый метод HTTP запроса:

```
GET
```

Путь, относительно базового URL:

```
/public/authentication?sid={{sid}}
```

Входные параметры в URL запроса:

Параметр	Тип данных	Обязательность	Описание
sid	UUID	Да	Внутренний идентификатор сессии, переданный в Адаптер (Запрос №4 на диаграмме взаимодействия (см. раздел **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**)).

Успешным ответом является возврат вызывающей стороне (User Agent пользователя) сформированного запроса для перенаправления на ЕСИА с целью аутентификации пользователя. Требования к данному запросу для перенаправления определены в Методических рекомендациях по работе с ЕСИА.

Пример запроса:

```
GET /servlets/api/v1/public/authentication?sid=0100e0f3-b662-4479-bc31-4ded6990d810
HTTP/1.1
Host: t01adaptertib01:9000
Authorization: Bearer SIGN
```

Пример ответа:

```
HTTP/1.1 302
Cache-Control: private
```

```
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: https://esia-
portal1.test.gosuslugi.ru/aas/oauth2/ac?access_type=offline&scope=openid%20bio&resp
onse_type=code&client_secret=MIIKZQYJKoZIhvcNAQcCoIIKVjCCClICAQExDDAKBgYqhQMCAgkFAD
ALBgkqhkiG9w0BBwGgggf/MIIH%2BzCCB6qgAwIBAgIRAXILAVZQABCz6BEFgeFMnQAwCAYGKoUDAgIDMII
BRjEYMBYGBSqFA2QBEg0xMjM0NTY3ODkwMTIzMRowGAYIKoUDA4EDAQESDDAwMTIzNDU2Nzg5MDEpMCcGA1
UECQwg0KHRg9GJ0LXQstGB0LrQuNC5INCy0LDQuyDQtC4gMjYxFzAVBgkqhkiG9w0BCQEWCGNhQHJ0LnJ1M
QswCQYDVQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB0LrQstCwMRUwEwYDVQQHDAzQnNC%2B0YHQutCy0L
AxJDAiBgNVBAoMG9Ce0JDQniDQoNC%2B0YHRgtC10LvQtdC60L7QvDEwMC4GA1UECwwn0KPQtNC%2B0YHRg
tC%2B0LLQtdGA0Y/RjtGJ0LjQuSDRhtC10L3RgtGAMTQwMgYDVQQDDCvQotC10YHRgtC%2B0LLRi9C5INCj
0KYg0KDQotCaICjQoNCi0JvQsNCx0YEpMB4XDTE4MDcwNjEwMDIwMVoXDTE5MDcwNjEwMTIwMVowggEuMRY
wFAYJKoZIhvcNAQkCDAdVQlNfREVWMSYwJAYJKoZIhvcNAQkBFhdNYXhpbS5rb21hcm92QHJ0bGFicy5ydT
EaMBgGCCqFAwOBAwEBEgwwMDc3MDcwNDkzODgxGDAWBgUqhQNkARINMTAyNzcwMDE5ODc2NzEmMCQGA1UEC
gwd0J/QkNCeICLQoNC%2B0YHRgtC10LvQtdC60L7QvCIxKjAoBgNVBAcMIdCzLiDQodCw0L3QutGCLdCf0L
XRgtC10YDQsdGD0YDQszEtMCsGA1UECAwkNzgg0LMuINCh0LDQvdC60YIt0J/QtdGC0LXRgNCx0YPRgNCzM
QswCQYDVQQGEwJSVTEmMCQGA1UEAwwd0J/QkNCeICLQoNC%2B0YHRgtC10LvQtdC60L7QvCIwYzAcBgYqhQ
MCAhMwEgYHKoUDAgIkAAYHKoUDAgIeAQNDAARAI6EpvwN0WxMFnLZJnOwyNkL3SGe1i6sb1JgsdNFlS1zXq
voq%2B802R8ErpHOmlN/Fa3TVAJkDZnwW5Dd3S7ybT6OCBIMwggR/MA4GA1UdDwEB/wQEAwIE8DAdBgNVHQ
4EFgQUJQ7mPvdGiNdtZjnts9RQqJJgmQAwggGIBgNVHSMEggF/MIIBe4AUPu8ZPw%2B5ebDx5ikho%2BS5l
bml7pChggFOpIIBSjCCAUYxGDAWBgUqhQNkARINMTIzNDU2Nzg5MDEyMzEaMBgGCCqFAwOBAwEBEgwwMDEy
MzQ1Njc4OTAxKTAnBgNVBAkMINCh0YPRidC10LLRgdC60LjQuSDQstCw0Lsg0LQuIDI2MRcwFQYJKoZIhvc
NAQkBFghjYUBydC5ydTELMAkGA1UEBhMCUlUxGDAWBgNVBAgMDzc3INCc0L7RgdC60LLQsDEVMBMGA1UEBw
wM0JzQvtGB0LrQstCwMSQwIgYDVQQKDBvQntCQ0J4g0KDQvtGB0YLQtdC70LXQutC%2B0LwxMDAuBgNVBAs
MJ9Cj0LTQvtGB0YLQvtCy0LXRgNGP0Y7RidC40Lkg0YbQtdC90YLRgDE0MDIGA1UEAwwr0KLQtdGB0YLQvt
Cy0YvQuSDQo9CmINCg0KLQmiAo0KDQotCb0LDQsdGBKYIRAXILAVZQALmz5xHPOr40d6AwHQYDVR0lBBYwF
AYIKwYBBQUHAwIGCCsGAQUFBwMEMCcGCSsGAQQBgjcVCgQaMBgwCgYIKwYBBQUHAwIwCgYIKwYBBQUHAwQw
HQYDVR0gBBYwFDAIBgYqhQNkcQEwCAYGKoUDZHECMCsGA1UdEAQkMCKADzIwMTgwNzA2MTAwMjAxWoEPMjA
xOTA3MDYxMDAyMDFaMIIBNAYFKoUDZHAEggEpMIIBJQwrItCa0YDQuNC/0YLQvtCf0YDQviBDU1AiICjQst
C10YDRgdC40Y8gMy45KQwsItCa0YDQuNC/0YLQvtCf0YDQviDQo9CmIiAo0LLQtdGA0YHQuNC4IDIuMCkMY
9Ch0LXRgNGC0LjRhNC40LrQsNGCINGB0L7QvtGC0LLQtdGC0YHRgtCy0LjRjyDQpNCh0JEg0KDQvtGB0YHQ
uNC4IOKEliDQodCkLzEyNC0yNTM5INC%2B0YIgMTUuMDEuMjAxNQxj0KHQtdGA0YLQuNGE0LjQutCw0YIg0
YHQvtC%2B0YLQstC10YLRgdGC0LLQuNGPINCk0KHQkSDQoNC%2B0YHRgdC40Lgg4oSWINCh0KQvMTI4LTI4
ODEg0L7RgiAxMi4wNC4yMDE2MDYGBSqFA2RvBC0MKyLQmtGA0LjQv9GC0L7Qn9GA0L4gQ1NQIiAo0LLQtdG
A0YHQuNGPIDMuOSkwZQYDVR0fBF4wXDBaoFigVoZUaHR0cDovL2NlcnRlbnJvbGwudGVzdC5nb3N1c2x1Z2
kucnUvY2RwLzNlZWYxOTNmMGZiOTc5YjBmMWU2MjkyMWEzZTRiOTk1YjlhNWVlOTAuY3JsMFcGCCsGAQUFB
wEBBEswSTBHBggrBgEFBQcwAoY7aHR0cDovL2NlcnRlbnJvbGwudGVzdC5nb3N1c2x1Z2kucnUvY2RwL3Rl
c3RfY2FfcnRsYWJzMi5jZXIwCAYGKoUDAgIDA0EAoUYc8UzU2SsFA%2BWo9Nkiqe%2Bg9WfNB6/zB8H1M1A
FypgcdmSqwiNuygc8Yk%2BrvpJR2baVI8gH43FT82Aq7HEbETGCAi0wggIpAgEBMIIBXTCCAUYxGDAWBgUq
```

```
hQNkARINMTIzNDU2Nzg5MDEyMzEaMBgGCCqFAwOBAwEBEgwwMDEyMzQ1Njc4OTAxKTAnBgNVBAkMINCh0YP
RidC10LLRgdC60LjQuSDQstCw0Lsg0LQuIDI2MRcwFQYJKoZIhvcNAQkBFghjYUBydC5ydTELMAkGA1UEBh
MCUlUxGDAWBgNVBAgMDzc3INCc0L7RgdC60LLQsDEVMBMGA1UEBwwM0JzQvtGB0LrQstCwMSQwIgYDVQQKD
BvQntCQ0J4g0KDQvtGB0YLQtdC70LXQutC%2B0LwxMDAuBgNVBAsMJ9Cj0LTQvtGB0YLQvtCy0LXRgNGP0Y
7RidC40Lkg0YbQtdC90YLRgDE0MDIGA1UEAwwr0KLQtdGB0YLQvtCy0YvQuSDQo9CmINCg0KLQmiAo0KDQo
tCb0LDQsdGBKQIRAXILAVZQABCz6BEFgeFMnQAwCgYGKoUDAgIJBQCgaTAYBgkqhkiG9w0BCQMxCwYJKoZI
hvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0xOTA0MjUxMTE2NDNaMC8GCSqGSIb3DQEJBDEiBCBmiWxRFhvwv%2
BXWEuu/h9/rTqgtnF8LX/jJj1mcklRG2DAKBgYqhQMCAhMFAARArOSy4sY5sSVdItvu1Sh2mSDZu6cGUKQ5
E5Fj72c/De8CVVyhM8PFOA863T2S/1Cx%2BmYkFzcZ4OIoqfythhpt1w%3D%3D&redirect_uri=http://
172.20.11.79:8787/servlets/api/v1/public/verification&state=0aed8c79-a575-3d54-
a6fe-133db91200ba&client_id=UBS_DEV&timestamp=2019.04.25%2011:16:42%20%2B0000
Set-Cookie: adapter=a30f8af2-4c4f-404a-b5b9-df7cd102c084
Content-Type: application/json
```

2.2.4.2.2 Функция "Получение доступа к биометрической верификации"

Запрос №5 на диаграмме взаимодействия (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Вызывается пользователем после успешного получения кода авторизации для scope="openid, bio" в ЕСИА. Клиенту передаются данные для перенаправления на ЕБС для проведения биометрической верификации пользователя (в рамках процесса удаленной идентификации).

Формат вызова определен в Методических рекомендациях по работе с ЕБС.

Пример запроса:

```
GET /servlets/api/v1/public/verification?state=1f412441-a661-48e9-bcdd-
fc4bc5edcaa3&code=eyJ2ZXIiOjEsInR5cCI6IkpXVCIsInNidCI6ImF1dGhvcml6YXRpb25fY29kZSIsI
mFsZyI6IkdPU1QzNDEwXzIwMTJfMjU2In0.eyJuYmYiOjE2OTg0MTY4MTcsInNjb3BlIjoiYmlvIG9wZW5p
ZCIsImF1dGhfdGltZSI6MTY5ODQxNjc1OCwiaXNzIjoiaHR0cDpcL1wvZXNpYS1wb3J0YWwxLnRlc3QuZ29
zdXNsdWdpLnJ1XC8iLCJ1cm46ZXNpYTpzaWQiOiJhYjkzZmUyMS0yYjg0LTRlMDktZmVjNy1jYmQ3OGNmZT
M1YmMiLCJ1cm46ZXNpYTpjbGllbnQ6c3RhdGUiOiIxZjQxMjQ0MS1hNjYxLTQ4ZTktYmNkZC1mYzRiYzVlZ
GNhYTMiLCJhdXRoX210aGQiOiJQV0QiLCJ1cm46ZXNpYTpzYmoiOnsidXJuOmVzaWE6c2JqOmx2bCI6IlBS
IiwidXJuOmVzaWE6c2JqOnR5cCI6IlAiLCJ1cm46ZXNpYTpzYmo6aXNfdHJ1Ijp0cnVlLCJ1cm46ZXNpYTp
zYmo6b2lkIjoxMDAwNzI0ODEzLCJ1cm46ZXNpYTpzYmo6bmFtIjoiT0lELjEwMDA3MjQ4MTMifSwiZXhwIj
oxNjk4NDE3MDU3LCJwYXJhbXMiOnt9LCJpYXQiOjE2OTg0MTY4MTcsImNsaWVudF9pZCI6IlJUSzAyMCJ9.
5pYWAV7PzMwV7QJYajEgyBeR9QrL7HGRRLLwB0MJ1_s2TWFJ0UcHJ7L1f1cHLIoacykRMkFWe1GE4fLawgu
DOw HTTP/1.1
Host: t01adaptertib01.tkur.ebsbio.tech:9000
Authorization: Bearer SIGN
Cookie: adapter=292fb210-698d-42a5-a5d2-cb1708100308
```

Пример ответа:

```
HTTP/1.1 302
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location:
https://int.ebs.ru/vrf?session_id=4810E65022314A7A9D21BAF43DB475E9&redirect=http%3A
%2F%2F172.20.11.79%3A8787%2Fservlets%2Fapi%2Fv1%2Fpublic%2Fresult%3Fstate%3D0aed8c7
9-a575-3d54-a6fe-133db91200ba
Content-Type: application/json
Content-Length: 0
Date: Thu, 25 Apr 2019 11:16:54 GM
```

2.2.4.2.3 Функция "Передача результата верификации"

Запрос №6 на диаграмме взаимодействия (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Вызывается пользователем после прохождения биометрической верификации в ЕБС (в рамках процесса удаленной идентификации). Успешным ответом является возврат вызывающей стороне (клиенту) сформированного запроса для перенаправления на ЕСИА с целью аутентификации пользователя.

Формат вызова определен в Методических рекомендациях по работе с ЕБС для разработчиков.

Пример запроса:

```
GET
/servlets/api/v1/public/result?state=1f412441-a661-48e9-bcdd-
fc4bc5edcaa3&expired=1992660627&verify_token=de0e9b33-2c67-449b-bc25-87d2f8b695e0
HTTP/1.1
Host: t01adaptertib01:9000
Cookie: adapter=292fb210-698d-42a5-a5d2-cb1708100308
```

Пример ответа:

```
HTTP/1.1 302
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: https://esia-
portal1.test.gosuslugi.ru/aas/oauth2/ac?access_type=offline&scope=openid%20ext_auth
_result&response_type=code&client_secret=MIIKZQYJKoZIhvcNAQcCoIIKVjCCClICAQExDDAKBg
YqhQMCAgkFADALBgkqhkiG9w0BBwGgggf/MIIH%2BzCCB6qgAwIBAgIRAXILAVZQABCz6BEFgeFMnQAwCAY
GKoUDAgIDMIIBRjEYMBYGBSqFA2QBEg0xMjM0NTY3ODkwMTIzMRowGAYIKoUDA4EDAQESDDAwMTIzNDU2Nz
g5MDEpMCcGA1UECQwg0KHRg9GJ0LXQstGB0LrQuNC5INCy0LDQuyDQtC4gMjYxFzAVBgkqhkiG9w0BCQEWC
GNhQHJ0LnJ1MQswCQYDVQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB0LrQstCwMRUwEwYDVQQHDAzQnNC%
```

2B0YHQutCy0LAxJDAiBgNVBAoMG9Ce0JDQniDQoNC%2B0YHRgtC10LvQtdC60L7QvDEwMC4GA1UECwwn0KP
QtNC%2B0YHRgtC%2B0LLQtdGA0Y/RjtGJ0LjQuSDRhtC10L3RgtGAMTQwMgYDVQQDDCvQotC10YHRgtC%2B
0LLRi9C5INCj0KYg0KDQotCaICjQoNCi0JvQsNCx0YEpMB4XDTE4MDcwNjEwMDIwMVoXDTE5MDcwNjEwMTI
wMVowggEuMRYwFAYJKoZIhvcNAQkCDAdVQlNfREVWMSYwJAYJKoZIhvcNAQkBFhdNYXhpbS5rb21hcm92QH
J0bGFicy5ydTEaMBgGCCqFAwOBAwEBEgwwMDc3MDcwNDkzODgxGDAWBgUqhQNkARINMTAyNzcwMDE5ODc2N
zEmMCQGA1UECgwd0J/QkNCeICLQoNC%2B0YHRgtC10LvQtdC60L7QvCIxKjAoBgNVBAcMIdCzLiDQodCw0L
3QutGCLdCf0LXRgtC10YDQsdGD0YDQszEtMCsGA1UECAwkNzgg0LMuINCh0LDQvdC60YIt0J/QtdGC0LXRg
NCx0YPRgNCzMQswCQYDVQQGEwJSVTEmMCQGA1UEAwwd0J/QkNCeICLQoNC%2B0YHRgtC10LvQtdC60L7QvC
IwYzAcBgYqhQMCAhMwEgYHKoUDAgIkAAYHKoUDAgIeAQNDAARAI6EpvwN0WxMFnLZJnOwyNkL3SGe1i6sb1
JgsdNFlS1zXqvoq%2B802R8ErpHOmlN/Fa3TVAJkDZnwW5Dd3S7ybT6OCBIMwggR/MA4GA1UdDwEB/wQEAw
IE8DAdBgNVHQ4EFgQUJQ7mPvdGiNdtZjnts9RQqJJgmQAwggGIBgNVHSMEggF/MIIBe4AUPu8ZPw%2B5ebD
x5ikho%2BS5lbml7pChggFOpIIBSjCCAUYxGDAWBgUqhQNkARINMTIzNDU2Nzg5MDEyMzEaMBgGCCqFAwOB
AwEBEgwwMDEyMzQ1Njc4OTAxKTAnBgNVBAkMINCh0YPRidC10LLRgdC60LjQuSDQstCw0Lsg0LQuIDI2MRc
wFQYJKoZIhvcNAQkBFghjYUBydC5ydTELMAkGA1UEBhMCUlUxGDAWBgNVBAgMDzc3INCc0L7RgdC60LLQsD
EVMBMGA1UEBwwM0JzQvtGB0LrQstCwMSQwIgYDVQQKDBvQntCQ0J4g0KDQvtGB0YLQtdC70LXQutC%2B0Lw
xMDAuBgNVBAsMJ9Cj0LTQvtGB0YLQvtCy0LXRgNGP0Y7RidC40Lkg0YbQtdC90YLRgDE0MDIGA1UEAwwr0K
LQtdGB0YLQvtCy0YvQuSDQo9CmINCg0KLQmiAo0KDQotCb0LDQsdGBKYIRAXILAVZQALmz5xHPOr40d6AwH
QYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMCcGCSsGAQQBgjcVCgQaMBgwCgYIKwYBBQUHAwIwCgYI
KwYBBQUHAwQwHQYDVR0gBBYwFDAIBgYqhQNkcQEwCAYGKoUDZHECMCsGA1UdEAQkMCKADzIwMTgwNzA2MTA
wMjAxWoEPMjAxOTA3MDYxMDAyMDFaMIIBNAYFKoUDZHAEggEpMIIBJQwrItCa0YDQuNC/0YLQvtCf0YDQvi
BDU1AiICjQstC10YDRgdC40Y8gMy45KQwsItCa0YDQuNC/0YLQvtCf0YDQviDQo9CmIiAo0LLQtdGA0YHQu
NC4IDIuMCkMY9Ch0LXRgNGC0LjRhNC40LrQsNGCINGB0L7QvtGC0LLQtdGC0YHRgtCy0LjRjyDQpNCh0JEg
0KDQvtGB0YHQuNC4IOKEliDQodCkLzEyNC0yNTM5INC%2B0YIgMTUuMDEuMjAxNQxj0KHQtdGA0YLQuNGE0
LjQutCw0YIg0YHQvtC%2B0YLQstC10YLRgdGC0LLQuNGPINCk0KHQkSDQoNC%2B0YHRgdC40Lgg4oSWINCh
0KQvMTI4LTI4ODEg0L7RgiAxMi4wNC4yMDE2MDYGBSqFA2RvBC0MKyLQmtGA0LjQv9GC0L7Qn9GA0L4gQ1N
QIiAo0LLQtdGA0YHQuNGPIDMuOSkwZQYDVR0fBF4wXDBaoFigVoZUaHR0cDovL2NlcnRlbnJvbGwudGVzdC
5nb3N1c2x1Z2kucnUvY2RwLzNlZWYxOTNmMGZiOTc5YjBmMWU2MjkyMWEzZTRiOTk1YjlhNWVlOTAuY3JsM
FcGCCsGAQUFBwEBBEswSTBHBggrBgEFBQcwAoY7aHR0cDovL2NlcnRlbnJvbGwudGVzdC5nb3N1c2x1Z2ku
cnUvY2RwL3Rlc3RfY2FfcnRsYWJzMi5jZXIwCAYGKoUDAgIDA0EAoUYc8UzU2SsFA%2BWo9Nkiqe%2Bg9Wf
NB6/zB8H1M1AFypgcdmSqwiNuygc8Yk%2BrvpJR2baVI8gH43FT82Aq7HEbETGCAi0wggIpAgEBMIIBXTCC
AUYxGDAWBgUqhQNkARINMTIzNDU2Nzg5MDEyMzEaMBgGCCqFAwOBAwEBEgwwMDEyMzQ1Njc4OTAxKTAnBgN
VBAkMINCh0YPRidC10LLRgdC60LjQuSDQstCw0Lsg0LQuIDI2MRcwFQYJKoZIhvcNAQkBFghjYUBydC5ydT
ELMAkGA1UEBhMCUlUxGDAWBgNVBAgMDzc3INCc0L7RgdC60LLQsDEVMBMGA1UEBwwM0JzQvtGB0LrQstCwM
SQwIgYDVQQKDBvQntCQ0J4g0KDQvtGB0YLQtdC70LXQutC%2B0LwxMDAuBgNVBAsMJ9Cj0LTQvtGB0YLQvt
Cy0LXRgNGP0Y7RidC40Lkg0YbQtdC90YLRgDE0MDIGA1UEAwwr0KLQtdGB0YLQvtCy0YvQuSDQo9CmINCg0
KLQmiAo0KDQotCb0LDQsdGBKQIRAXILAVZQABCz6BEFgeFMnQAwCgYGKoUDAgIJBQCgaTAYBgkqhkiG9w0B
CQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0xOTA0MjUxMTE5MDNaMC8GCSqGSIb3DQEJBDEiBCA
D66o90NFwqDHZ4gDml/1PI28cbA/ymPY7CahnQgHPoTAKBgYqhQMCAhMFAARAw3/v6CBJVH2o4FRfIY0msr

```
vDQHULsOsD9pH4seOUIKEjOt8LFQCoH00LuXyACkJwqnzHatnKVedrnaSVqyIHNg%3D%3D&redirect_uri
=http://172.20.11.79:8787/servlets/api/v1/public/end&state=0aed8c79-a575-3d54-a6fe-
133db91200ba&verify_token=465bc787-661b-4671-b520-
9c93daeb8a68&client_id=UBS_DEV&timestamp=2019.04.25%2011:19:03%20%2B0000
Content-Type: application/json
Content-Length: 0
```

2.2.4.2.4 Функция "Получение параметра успешного завершения"

Запрос №7 на диаграмме взаимодействия (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Вызывается пользователем после успешного получения кода авторизации для scope="openid, ext_auth_result" в ЕСИА (в рамках процесса удаленной идентификации). Результатом является возврат пользователю (в МП КА или браузере) специального параметра res_secret, который пользователь далее предъявляет ИС КА для выполнения бизнес-операции в ИС КА аутентифицированным образом.

Формат вызова определен в Методических рекомендациях по работе с ЕБС для разработчиков.

Пример запроса на получение параметра успешного завершения:

```
GET
/servlets/api/v1/public/end?code=eyJ2ZXIiOjEsInR5cCI6IkpXVCIsInNidCI6ImF1dGhvcml6YX
Rpb25fY29kZSIsImFsZyI6IkdPU1QzNDEwIn0.eyJuYmYiOjE1NTYxOTExNDMsInNjb3BlIjoiZXh0X2F1d
GhfcmVzdWx0P29pZD0xMDAwMzE2OTEwIG9wZW5pZCIsImF1dGhfdGltZSI6MTU1NjE5MTAwOCwiaXNzIjoi
aHR0cDpcL1wvZXNpYS5nb3N1c2x1Z2kucnVcLyIsInVybjplc2lhOnNpZCI6ImU0ZDlkNjYzY2NiMmM4MDQ
4Mjc0MWQ2ZDk3ZTMwZmFkMDZiMjc0MTkwYzUyOWRiMjhiOGYyZmFiZGYwMzVmNmUiLCJ1cm46ZXNpYTpjbG
llbnQ6c3RhdGUiOiIwYWVkOGM3OS1hNTc1LTNkNTQtYTZmZS0xMzNkYjkxMjAwYmEiLCJhdXRoX210aGQiO
iJQV0QiLCJ1cm46ZXNpYTpzYmoiOnsidXJuOmVzaWE6c2JqOnR5cCI6IlAiLCJ1cm46ZXNpYTpzYmo6aXNf
dHJ1Ijp0cnVlLCJ1cm46ZXNpYTpzYmo6b2lkIjoxMDAwMzE2OTEwLCJ1cm46ZXNpYTpzYmo6bmFtIjoiT0l
ELjEwMDAzMTY5MTAiLCJ1cm46ZXNpYTpzYmo6ZWlkIjo3NDMxNzg3fSwiZXhwIjoxNTU2MTkxMzgzLCJwYX
JhbXMiOnsicmVtb3RlX2lwIjoiMTAuNjguMzUuMjYiLCJ1c2VyX2FnZW50IjoiTW96aWxsYVwvNS4wIChXa
W5kb3dzIE5UIDEwLjA7IFdpbjY0OyB4NjQpIEFwcGxlV2ViS2l0XC81MzcuMzYgKEtIVE1MLCBsaWtlIEdl
Y2tvKSBDaHJvbWVcLzY1LjAuMzMyNS4xNDYgU2FmYXJpXC81MzcuMzYifSwiaWF0IjoxNTU2MTkxMTQzLCJ
jbGllbnRfaWQiOiJVQlNfREVWIn0.3S9H4Kpa8U_SeGxYwRRUrt8yctYT-4jnnwoPJBMRx1EE3sSolfo-
YoDfgu6jINFke0Wn6R2RAqiZid7UQ7eWaQ&state=0aed8c79-a575-3d54-a6fe-133db91200ba
HTTP/1.1
Host: 172.20.11.79:8787
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
```

```
like Gecko) Chrome/65.0.3325.146 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
.8
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: adapter=a30f8af2-4c4f-404a-b5b9-df7cd102c084
```

Пример ответа на запрос получения параметра успешного завершения:

```
HTTP/1.1 302
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: http://d00nbphdp03:8281/?res_secret=c1fa69ac-6a73-427e-974b-ebf9431cfb3c
Content-Type: application/json
Content-Length: 0
Date: Thu, 25 Apr 2019 11:19:04 GMT
```

Пример запроса передачи пользователем в ИС КА параметра res_secret (запрос на завершение процесса):

```
GET /?res_secret=c1fa69ac-6a73-427e-974b-ebf9431cfb3c HTTP/1.1
Host: d00nbphdp03:8281
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/65.0.3325.146 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
.8
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
```

Пример ответа передачи пользователем в ИС КА параметра res_secret:

```
HTTP/1.1 200 OK
Date: Thu, 25 Apr 2019 11:19:04 GMT
Connection: keep-alive
Transfer-Encoding: chunked
```

2.2.4.3 Спецификация API получения результата верификации ИС КА

ИС КА должна реализовать функцию данного API. Функция используется Адаптером для передачи в ИС КА результата выполнения протокола удаленной идентификации с использованием ЕСИА и ЕБС, ПДн пользователя. Вызовы осуществляются в пределах контролируемой зоны КА.

В случае успешного выполнения протокола, в ИС КА передается результат удаленной идентификации, ПДн пользователя, специальный параметр "res_secret", который пользователь предъявляет ИС КА для выполнения бизнес-операции в ИС КА аутентифицированным образом.

В случае возникновения ошибки в процессе выполнения протокола удаленной идентификации Адаптер передает в ИС КА код и описание ошибки.

Прикладные ошибки, которые Адаптер может вернуть в ИС КА:

Значение параметра «code»	**Описание (параметр «message»)**
ADR-0000	Внутренняя ошибка API
ADR-0001	Запрос не содержит обязательного параметра
ADR-0002	Неверные параметры запроса
ADR-0201	Ошибка формирования ЭП для запроса в ЕСИА
ADR-0204	Истекло время жизни сессии
ADR-0205	Внутренняя ошибка при работе с базой данных
ADR-0206	Попытка перехода сессии пользователя в запрещенное состояние
ADR-0207	Ошибка при отправке запроса в ЕСИА
ADR-0208	Получено сообщение об ошибке от ЕСИА
ADR-0209	Ошибка формата данных полученных из ЕСИА
ADR-0210	Ошибка отправки запроса в ЕБС
ADR-0211	Получено сообщение об ошибке от ЕБС
ADR-0212	Ошибка формата данных полученных из ЕБС

2.2.4.3.1 Функция "Получение результата удаленной идентификации"

Запрос №8 на диаграмме взаимодействия (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Адаптер вызывает данную функцию для передачи в ИС КА результата выполнения протокола аутентификации с использованием ЕСИА и ЕБС, ПДн пользователя.

Адаптер осуществляет вызов на URL, переданный ИС КА в параметре dbo_ko_uri при вызове функции Адаптера "Создание сессии в Адаптере" (Запрос №2 на диаграмме взаимодействия (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**)).

Поддерживаемый метод HTTP запроса:

```
POST
```

URL запроса к данной функции API ИС КА:

```
{{dbo_ko_uri}},
```

где {{dbo_ko_uri}} - URL "API получения результата верификации ИС КА", который был передан Адаптеру от ИС КА при вызове функции "Создание сессии в Адаптере" (см. раздел **Ошибка! Источник ссылки не найден.**) в контексте сессии с идентификатором sid.

Заголовки запроса:

```
Content-Type: application/json
```

Входные параметры в теле запроса в формате JSON:

Параметр	Тип данных	Обязательность	Описание
sid	UUID	Да	Обязательный параметр. Идентификатор сессии
auth_result	Булево выражение	Да	Обязательный параметр. Результат процесса удаленной идентификации с использованием ЕСИА и ЕБС
code	Строка	Нет	Необязательный параметр. Присутствует только в случае возникновения ошибки выполнения процесса удаленной идентификации с использованием ЕСИА и ЕБС. Код ошибки.
message	Строка	Нет	Необязательный параметр. Присутствует только в случае возникновения ошибки выполнения процесса удаленной идентификации с использованием ЕСИА и ЕБС. Описание ошибки.
res_secret	Строка	Нет	Необязательный параметр. Присутствует только в случае успешного прохождения пользователем процесса удаленной идентификации с использованием ЕСИА и ЕБС. Параметр, с использованием которого далее происходит взаимодействие пользователя и КА
ext_auth_result	Строка	Нет	Необязательный параметр. Присутствует только в случае успешного прохождения пользователем процесса удаленной идентификации с использованием ЕСИА и ЕБС. Расширенный результат верификации, полученный от ЕБС, содержащий степени схожести (общая и по каждой из модальностей). Параметр передается в формате JWT токена.
person_data	Массив	Нет	Необязательный параметр. Присутствует только в случае успешного прохождения пользователем процесса удаленной идентификации с использованием ЕСИА и ЕБС. Набор ПДн пользователя из ЕСИА передается (при наличии) в рамках Постановления Правительства РФ от 10 июля 2013 г. N 584 "Об использовании федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

Успешный ответ: выходные параметры отсутствуют.

Пример запроса в случае возникновения ошибки выполнения процесса удаленной идентификации с использованием ЕСИА и ЕБС:

```
POST /api/dbo_ko_uri_path HTTP/1.1
```

```
Content-Type: application/json


{
  "sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
  "auth_result": false,
  "code": "ADR-0001",
  "message": "Запрос не содержит обязательного параметра"
}
```

Пример запроса в случае успешного прохождения пользователем процесса удаленной идентификации с использованием ЕСИА и ЕБС:

```
POST /api/dbo_ko_uri_path HTTP/1.1
Content-Type: application/json


{
  "sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
  "auth_result": true,
  "res_secret": "81ec6a78-26e5-438e-a6d4-1f15d91c9d7c",
  "ext_auth_result": "
eyJraWQiOiIyNTE4ZDNhMy05NTc0LTRkOTMtODQ0YS0wZjIwNjE2YTI3MjQiLCJ0eXAiOiJKV1QiLCJhbGc
iOiJHT1NUMzQxMCJ9.eyJyZXN1bHQiOnRydWUsInN1YiI6IjEwMDAzMTY5MTEiLCJhdWQiOiJUS19VQlNfR
EVWIiwibmJmIjoxNTUzMDAxNjgxLCJpc3MiOiJVQlNfREVWIiwibWF0Y2giOiJ7XCJvdmVyYWxsXCI6MS4w
LFwiZmFjZVwiOjEuMCxcInZvaWNlXCI6MS4wfSIsImV4cCI6MTU1MzAwMjI4MiwiaWF0IjoxNTUzMDAxNjg
wfQ==.BxQtSa5H7xpEZ_n8xiyy1F1D-
RiQDCDFGnucN6GCkmBKOwY0AxxNEl8TTN9wLNoYGBcEmD1RPNQhrDe45pHFgA==",
        "person_data": {
    "lastName": "Иванов",
    "addresses": {
        "stateFacts": ["hasSize"],
        "size": 2,
        "eTag": "EDBE4592683C4BC61B17D5100BE462A00504A99D",
        "elements": [{
                "stateFacts": ["Identifiable"],
                "id": 626
                21,
                "type": "PLV",
                "countryId": "RUS",
                "addressStr": "г Иркутск, ул 2-я Московская",
                "fiasCode": "65d77bbf-d002-4ecd-8390-583ccfdbf034",
```

```
                "zipCode": "664014",
                "region": "Иркутская",
                "city": "Иркутск",
                "street": "2-я Московская",
                "house": "77",
                "eTag": "1DFABE9B957174C89E6FAE6132F6FC9D
                5071E5F8"
            }, {
                "stateFacts": ["Identifiable"],
                "id": 62620,
                "type": "PRG",
                "countryId": "RUS",
                "addressStr": "г Воронеж, ул Московская",
                "fiasCode": "fc60c716-57f2-461a-8a21-52d6a7d650a4",
                "zipCode": "394018",
                "region": "Воронежская",
                "city": "Воронеж",
                "street": "Московская",
                "house":
                "1",
                "eTag": "55730F91FF9B78767C105A0E5A09D31585C1496F"
            }
        ]
    },
    "verifying": false,
    "gender": "M",
    "documents": {
        "stateFacts": ["hasSize"],
        "size": 1,
        "eTag": "2778A43AB950AE02B8E8EC2CC8402E14E28C7C23",
        "elements": [{
                "stateFacts": ["EntityRoot"],
                "id": 35801,
                "type": "RF_PASSPORT",
                "vrfS
                tu": "VERIFIED",
                "series": "1000",
                "number": "200300",
```

```
            "issueDate": "10.10.2010",
            "issueId": "360005",
            "issuedBy": "ОВД по Центральному району г. Воронеж",
            "eTag": "EEA78C891874184E92214C3D8AA5782330CB6AC7"
        }
    ]
},
"citizenship": "RUS",
"inn": "645933077752",
"updatedOn": 16125
47779,
"birthDate": "10.04.1992",
"stateFacts": ["EntityRoot"],
"rIdDoc": 35001,
"firstName": "Евгений",
"birthPlace": "г. Иркутск",
"trusted": true,
"containsUpCfmCode": false,
"middleName": "Владимирович",
"eTag": "1193F6F084C35136D8845769C42DC5842CAF1E16",
"snils": "000-000-000 31",
"
contacts": {
    "stateFacts": ["hasSize"],
    "size": 2,
    "eTag": "FBCF47412B3E5F724419371B9745CE6A77D6C098",
    "elements": [{
            "stateFacts": ["Identifiable"],
            "id": 14276100,
            "type": "EML",
            "vrfStu": "VERIFIED",
            "value": "esldff@gmail.com",
            "eTag": "1D2E54819C4D9676FED052DC52C9EC4AF5D75522"
        }, {
            "stateFacts": ["Identifiable"],
            "id": 14446190,
            "type": "MBT",
            "vrfStu": "VERIFIED",
```

```
                "value": "+7(999)5888000",
                "eTag": "2FE8A73E9A89BAA5B9C334B9FCC7BE26E2FAB6CE"
            }
        ]
    },
    "status": "REGISTERED"
}
}
```

Пример ответа ИС КА:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
```

Прикладные ошибки на стороне ИС КА (реализует ИС КА):

Код ответа HTTP	Значение параметра «code»	Описание (параметр «message»)
500	BNK-0000	Внутренняя ошибка ИС КА
400	BNK-0001	Запрос не содержит обязательного параметра
400	BNK-0002	Неверные параметры запроса
400	BNK-0003	Сессия с указанным sid не существует

2.2.4.4 Спецификация API верификации ИС КА, вызываемого пользовательскими устройствами

ИС КА должна реализовать функцию данного API. Вызовы функции осуществляются из сети Интернет от User Agent пользователя.

2.2.4.4.1 Функция "Возврат пользователя в ИС КА"

Функция используется Адаптером для перенаправления (возврата) User Agent пользователя в ИС КА в случае успешного выполнения протокола или возникновения ошибки.

Для перенаправления пользователя Адаптер возвращается HTTP-код 302. В заголовке Location указан URL, на который требуется перенаправить пользователя и необходимые параметры.

Адаптер осуществляет перенаправление на URL, переданный ИС КА в параметре dbo_ko_public_uri при вызове функции Адаптера "Создание сессии в Адаптере" (Запрос №2 на диаграмме взаимодействия (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**)).

В случае успешного выполнения протокола, в ИС КА передается результат удаленной идентификации, ПДн пользователя, специальный параметр "res_secret", который пользователь предъявляет ИС КА для выполнения бизнес-операции в ИС КА аутентифицированным образом.

Заголовок Location:

```
{{dbo_ko_public_uri}}?res_secret={{res_secret}},
```

где {{res_secret}} - параметр успешного завершения протокола.

Пример запроса в случае успешного завершения протокола удаленной идентификации:

```
HTTP/1.1 302 Found
Location: {{dbo_ko_public_uri}}?res_secret=81ec6a78-26e5-438e-a6d4-1f15d91c9d7c
```

В случае возникновения ошибки в процессе выполнения протокола удаленной идентификации Адаптер передает в ИС КА код и описание ошибки (см. п. 2.2.4.3.1, функция "Получение результата удаленной идентификации"). Затем Адаптер перенаправляет пользователя на публичный URL, переданный ИС КА в параметре dbo_ko_public_uri.

Заголовок Location:

```
{{dbo_ko_public_uri}}?sid={{sid}},
```

где {{sid}} - идентификатор сессии пользователя (см. п. 2.2.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Пример запроса (перенаправления пользователя на dbo_ko_public_uri), если удаленная идентификация завершилась с ошибкой и код ошибки был успешно передан в ИС КА (см. п. 2.2.4.3):

```
HTTP/1.1 302 Found
Location: {{dbo_ko_public_uri}}?sid=5b9dcd00-71a6-4293-ac6c-f367a2ebef7f
```

В случае, если передача кода и описания ошибки в ИС КА (см. п. 2.2.4.3, функция "Получение результата удаленной идентификации") завершилась с ошибкой, Адаптер в заголовке Location передает дополнительный параметр "code", значение которого равно "ADR-0004".

Заголовок Location:

```
{{dbo_ko_public_uri}}?sid={{sid}}&{{code}},
```

где {{sid}} - идентификатор сессии пользователя (см. п. 2.1.1, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**), а

{{code}} - признак неудачной отправки кода и описания ошибки в ИС КА "ADR-0004".

Пример запроса (перенаправления пользователя на dbo_ko_public_uri), если удаленная идентификация завершилась с ошибкой и код ошибки не был передан в ИС КА (ИС КА не ответил или ответил с ошибкой):

```
HTTP/1.1 302 Found
Location: {{dbo_ko_public_uri}}?sid=5b9dcd00-71a6-4293-ac6c-f367a2ebef7f&code=ADR-
0004
```

где "ADR-0004" - код ошибки отправки результата в ИС КА.

2.2.5 Внутренний API Адаптера для биометрической регистрации (через СМЭВ)

API используется ИС КА для:

- подписания биометрических образцов перед отправкой в ВС ЕБС на СМЭВ 3.
- подписания запросов на поиск и регистрацию УЗ клиента в ЕСИА (ВС ЕСИА на СМЭВ 3);
- проверки ЭП СМЭВ 3.

Вызовы осуществляются в пределах контролируемой зоны КА.

Интерфейсы, их схема взаимодействия и коды возврата могут уточняться на этапе разработки и проведения исследований, предусмотренных настоящим документом.

Реализация

Аспект реализации	Реализация
Транспортный протокол	HTTPS
Аутентификация вызывающей стороны	Authorization - обязательный заголовок в запросе. Имеет вид Authorization: Bearer токен_доступа. Токен доступа прописывается в конфигурации адаптера и выдается ППО ИС КА.

2.2.5.1 Функция «Подписать сообщение для СМЭВ 3»

Функция принимает на вход:

- СМЭВ-конверт с запросом сведений;
- от нуля до N (параметр конфигурации Адаптера, определяется видом сведений ЕБС на СМЭВ 3) вложений (подписываемые данные), если требуется ЭП СМЭВ-конверта с запросом вида сведений ЕБС.

Функция поддерживает три типа СМЭВ-конвертов (тип сообщения для СМЭВ):

- SendRequestRequest
- AckRequest
- GetResponseRequest

ИС КА предварительно должна сформировать все необходимые служебные блоки СМЭВ 3, блок запроса ВС (при передаче SendRequestRequest) и провести все необходимые канонизации и трансформации XML.

Функция при получении СМЭВ-конверта вида SendRequestRequest:

- проводит аутентификацию вызывающей стороны по токену доступа в заголовке Authorization;
- определяет соответствующий токену доступа ключевой контейнер, сертификат;
- проверяет целевое использование Адаптера путем контроля идентификатора ВС ЕБС или ВС ЕСИА в СМЭВ-конверте с запросом сведений.
- для каждого передаваемого вложения (параметр attachment) проверяет соответствие идентификатора вложения, указанного в атрибуте тэга "AttachmentRef", идентификатору, указанному в атрибуте name заголовка "Content-Disposition" части multipart;
- для каждого передаваемого вложения считается хэш и ЭП в формате PKCS#7;
- идентификаторы вложений и соответствующие им хэш, ЭП в формате PKCS#7 включаются в блок заголовков и ЭП вложений ("RefAttachmentHeaderList");

- блок "SenderProvidedRequestData", включающий в себя запрос ВС (блок "MessagePrimaryContent"), блок заголовков и ЭП вложений (блок "RefAttachmentHeaderList") и служебные блоки СМЭВ 3 (формирутся ИС КА), подписывается ЭП в формате XML Dsig (Адаптер формирует блок ЭП " CallerInformationSystemSignature");
- готовый к отправке (подписанный ЭП) блок "SendRequestRequest" возвращается ИС КА.

Функция при получении СМЭВ-конверта вида AckRequest:

- проводит аутентификацию вызывающей стороны по токену доступа в заголовке Authorization;
- определяет соответствующий токену доступа ключевой контейнер, сертификат;
- блок "AckTargetMessage" (формируется ИС КА) подписывается ЭП в формате XML Dsig (Адаптер формирует блок ЭП " CallerInformationSystemSignature");
- готовый к отправке (подписанный ЭП) блок "AckRequest" возвращается ИС КА.

Функция при получении СМЭВ-конверта вида GetResponseRequest:

- проводит аутентификацию вызывающей стороны по токену доступа в заголовке Authorization;
- определяет соответствующий токену доступа ключевой контейнер, сертификат;
- блок "MessageTypeSelector" (формируется ИС КА) подписывается ЭП в формате XML Dsig (Адаптер формирует блок ЭП " CallerInformationSystemSignature");
- готовый к отправке (подписанный ЭП) блок "GetResponseRequest" возвращается ИС КА.

Требования к обрабатываемым XML:

- тип сообщения для СМЭВ: SendRequestRequest, AckRequest или GetResponseRequest;
- для SendRequestRequest:
  - В XML должны быть представлены блоки AttachmentRef с атрибутом attachmentId; условие нужно соблюдать, если на проверку пришли вложения и данные представляют собой ВС "Прием заявлений на биометрическую регистрацию";
  - оригинальная XML должна содержать непустой блок MessagePrimaryContent;
  - в переданной XML необходимо наличие блока SenderProvidedRequestData;
  - верхний блок переданной XML (которая содержит тип отправляемого СМЭВ-конверта) должна содержать атрибут xmlns:ns2, содержащий namespace-ссылку на типы сообщений СМЭВ (например, urn://x-artefacts-

smev-gov-ru/services/message-exchange/types/basic/1.2);

- для AckRequest:
  - в переданной XML необходимо наличие блока AckTargetMessage как дочерний элемент корневого блока;
- для GetResponseRequest:
  - в переданном блоке необходимо наличие блока MessageTypeSelector как дочерний элемент корневого блока.

Поддерживаемый метод HTTP запроса: POST

Путь, относительно базового URL: /reg/sign

Примечание: Запрос выполняется к модулю inner-smev-service и, в дополнение к базовому URL, должен содержать порт и контекст данного сервиса: 8082/inner-smev-service/ Например: https://{{adapter_url}}:8082/inner-smev-service/api/v1/reg/sign

Заголовки запроса:

```
Authorization: Bearer {{token}}
Content-Type: multipart/form-data,
```

где {{token}} - токен доступа ИС КА к API.

Входные параметры:

Параметр	Тип данных	Обязательность	Описание
xml_payload	Часть multipart, application/xml	Да	СМЭВ-конверт запросом сведений, которое ИС потребителя передает в СМЭВ (соответствующий блок) в формате XML.
attachment	Часть multipart, двоичные данные вложения, Content-Type зависит от типа передаваемого вложения.	Обязательный при запросе ВС ЕБС	Передается вместе с СМЭВ-конвертом вида SendRequestRequest и ВС "Прием заявлений на биометрическую регистрацию". Подписываемые данные (биометрический образец модальности "Голос", "Изображение лица"). Список частей multipart/form-data с заголовками в виде UUID вложения, указанного в передаваемом XML. Список UUID частей запроса должен совпадать с указанным списком UUID вложений в XML. Каждая часть содержит файл вложения, которое нужно будет подписать. Также каждая часть должна содержать соответствующий Content-Type вложения.

Выходные параметры успешного ответа:

Параметр	Тип данных	Обязательность	Описание
signature	application/xml	Да	Готовый к отправке (подписанный ЭП) XML.

Пример запроса:

```
POST /signer/api/v1/vrf/sign HTTP/1.1
Host: t01adaptertib01:5003
Content-Type: application/octet-stream
Authorization: Bearer te9c4a7-cer
```

```
Content-Length: 22

"<binary массив >"
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
"<binary массив… 230127111200Z
240127112200Z0,b10*…————————————————————d
————————————————————————————————————————————————————————————————————————————
77070493881-0+    *†H†ч
      -РђРґР°РїС,РµСЂ РўР□Р‘ С,РµСЃС,10*…————————————————————————d
10277001987671&0$————————————————————U
————————————————————————————————————————————————————————————————————————————
РµРђРћ
"Р PsCЃC,РµР»РµРєPsPj"1L0J————————————————————U
————————————————————————————————————————————————————————————————————————————
      СРЎРёРSPsРїСЃРєР°СЏ PSP°Р±РµСЂРµР¶PSP°СЏ, РґPsPj 14, Р»РёС,РµСЂ°
Рђ1*0(————————————————————U
————————————————————————————————————————————————————————————————————————————
!Pi. РЎР°PSPєС,-
РµРµС,РµСЂР±СѓСЂPi1)0'————————————————————U
————————————————————————————————————————————————————————————————————————————
78 РЎР°PSPєС,-РµРµС,РµСЂР±СѓСЂPi1
0
      ————————————————————U
————————————————————————————————————————————————————————————————————————————
RU1&0$————————————————————U
————————————————————————————————————————————————————————————————————————————
————————————————————РµРђРћ "Р PsCЃC,РµР»РµРєPsPj"0f0*…————————————————————
0
*…————————————————————$ *…————————————————————
————————————————————C
————————————————————————————————————————————————————————————————————————————
@KO$,N}`Ї5МћmOЉi=O{D@/<~Л"~шР36‰µ2,k7Й4JПv7ґлР[Э-ЮХ©эg
ЦжJ,>0,:0————————————————————Uя
————————————————————————————————————————————————————————————————————————————
————————————————————————————————————————————————————————————————————————————
————————————————————
————————————————————————————————————————————————————————————————————————————
p0————————————————————U
————————————————————————————————————————————————————————————————————————————
————————————————————————————————————————————————————————————————————————————
ЦВшч{€Е'"|VДп6[-
б°0————————————————————U%
————————————————————————————————————————————————————————————————————————————
0+————————————————————+————————————————————
————————————————————————————————————————————————————————————————————————————
0Ѓ§+
```

```
Ґљ0Ґ—
0D+0†8http://certenroll.test.gosuslugi.ru/cdp/test_ca_rtk2.cer0O+0†Chttp://testcara
/ra/aia/4d34315f0677fbedbc7c76f9878c72bacd3fa23a.crt0————————————————————U
00*…————————————————dq0*…————————————————dq0+
————————————————U
$0"Ђ20230127111159ZЃ2024012711115 9Z0,0*…————————————————dp
,%0,!+"РљСЂРёРїС,РsРµСЂРs CSP" (PIPµCЂCЃРёСЦ 4.0),"РљСЂРёРїС,РsРµСЂРs PJP¦"
(PIPµCЂCЃРёРё 2.0)aРЎРµСЂС,РёС„РёРєР°С,С‹ СЃРsРsС,PIPµС,СЃС,PIPёСЦ Р¤РЎР'
Р PsСЃСЃРёРё РЎР¤/124-3612 PsС, 10.01.2019aРЎРµСЂС,РёС„РёРєР°С,С‹
СЃРsРsС,PIPµС,СЃС,PIPёСЦ Р¤РЎР' Р PsСЃСЃРёРё РЎР¤/128-3592 PsС,
17.10.201806*…————————————————do
-+"РљСЂРёРїС,РsРµСЂРs CSP" (PIPµCЂCЃРёСЦ 4.0)0Ґ I————————————————U
… >"
```

Прикладные ошибки:

Код ответа HTTP	Значение параметра «code»	Описание ошибки
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа
400	ADR-0100	Недопустимый вид сведений
400	ADR-0101	Неверные идентификаторы вложений. Идентификаторы вложений не соответствуют XML запроса
400	ADR-0102	Представлена невалидная XML
400	ADR-0104	Передан неверный тип XML на подпись (разрешенный тип сообщения для СМЭВ)

2.2.5.2 Функция «Проверить подпись»

Функция принимает на вход:

- СМЭВ-конверт с ответом, который ИС КА получает из СМЭВ;
- СМЭВ-конверт с ответом о статусе ранее отправленного в СМЭВ сообщения, которое ИС КА получает из СМЭВ.

Функция выполняет следующее:

- проводит аутентификацию вызывающей стороны по токену доступа в заголовке Authorization;
- по полученной XML определяет тип XML, алгоритм подписи данных и получает сертификат;
- проводит проверку сертификата по цепочке в соотвествии с разделом 2.3.1;
- проводит проверку подписи в XML.

Функция возвращает результат проверки ЭП СМЭВ, содержащейся в СМЭВ-конверте. При проверке ЭП Адаптер проводит проверки актуальности сертификатов при помощи COC и OCSP-служб.

Требования к обрабатываемым XML:

- тип сообщения для СМЭВ: GetResponseResponse и SendRequestResponse;
- для GetResponseResponse:
  - должен присутствовать непустой дочерний блок (относительно корня переданной XML) ResponseMessage;
  - внутри блока ResponseMessage должны присутствовать заполненные блоки Response и SMEVSignature;
- для SendRequestResponse:
  - должны присутствовать заполненные дочерние блоки (относительно корня переданной XML) MessageMetadata и SMEVSignature.

Поддерживаемый метод HTTP запроса:

```
POST
```

Путь, относительно базового URL: /reg/verify

Примечание: Запрос выполняется к модулю inner-smev-service и, в дополнение к базовому URL, должен содержать порт и контекст данного сервиса: 8082/inner-smev-service/ Например: https://{{adapter_url}}:8082/inner-smev-service/api/v1/reg/verify

Заголовки запроса:

```
Authorization: Bearer {{token}},
```

где {{token}} - токен доступа ИС КА к API.

Входные параметры в теле запроса в формате application/xml:

Параметр	Тип данных	Обязательность	Описание
xml_payload	application/xml	Да	СМЭВ-конверт (XML блок "GetResponseResponse" или "SendRequestResponse"), ЭП которого необходимо проверить.

Выходные параметры успешного ответа:

Параметр	Тип данных	Обязательность	Описание
result	Булево выражение	Да	Результат проверки ЭП
message	Строка	Нет	Описание результата

Пример запроса:

```
POST /api/v1/reg/verify HTTP/1.1
Authorization: Bearer FAEA055D4EE948CEA031ACE10ECDAE49
Content-Type: application/xml

<ns2:SendRequestResponse xmlns="urn://x-artefacts-smev-gov-ru/services/message-
exchange/types/basic/1.2" xmlns:ns2="urn://x-artefacts-smev-gov-
ru/services/message-exchange/types/1.2" xmlns:ns3="urn://x-artefacts-smev-gov-
ru/services/message-exchange/types/faults/1.2"><ns2:MessageMetadata
Id="SIGNED_BY_SMEV"><ns2:MessageId>4c41a214-43d7-11e9-933a-
525400737462</ns2:MessageId><ns2:MessageType>REQUEST</ns2:MessageType><ns2:Sender><
ns2:Mnemonic>RTK02_3R</ns2:Mnemonic></ns2:Sender><ns2:SendingTimestamp>2019-03-
11T11:25:59.000+03:00</ns2:SendingTimestamp><ns2:Recipient><ns2:Mnemonic>RTK01_3R</
ns2:Mnemonic></ns2:Recipient><ns2:Status>requestIsQueued</ns2:Status></ns2:MessageM
etadata><ns2:SMEVSignature><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMe
thod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-
gostr3411"/><ds:Reference URI="#SIGNED_BY_SMEV"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:Transform
Algorithm="urn://smev-gov-ru/xmldsig/transform"/></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-
more#gostr3411"/><ds:DigestValue>pcmmYGmYHntCkdrRD4ICBcFJKNwmLqv+Pv3ja1//Vjk=</ds:D
igestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>ZTkM8zPI9ght+tkarw9jDU
yzm4Xwo1jwErVBH0BfZ24YBBNk3zJxERtbZJkjLvh3As7mE+B7E8n6dB2SRLWOQA==</ds:SignatureVal
ue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIIH2DCCB4egAwIBAgIRAXILAVZQABCz6RG
APpV5agEwCAYGKoUDAgIDMIIBRjEYMBYGBSqFA2QBEg0xMjM0NTY3ODkwMTIzMRowGAYIKoUDA4EDAQESDD
AwMTIzNDU2Nzg5MDEpMCcGA1UECQwg0KHRg9GJ0LXQstGB0LrQuNC5INCy0LDQuyDQtC4gMjYxFzAVBgkqh
kiG9w0BCQEWCGNhQHJ0LnJ1MQswCQYDVQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB0LrQstCwMRUwEwYD
VQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoMG9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEwMC4GA1U
ECwwn0KPQtNC+0YHRgtC+0LLQtdGA0Y/RjtGJ0LjQuSDRhtC10L3RgtGAMTQwMgYDVQQDDCvQotC10YHRgt
C+0LLRi9C5INCj0KYg0KDQotCaICjQoNCi0JvQsNCx0YEpMB4XDTE5MDMwNDEzMDg0MFoXDTIwMDMwNDEzM
Tg0MFowggELMR8wHQYJKoZIhvcNAQkCDBDQotCh0JzQrdCSM1/QmtCaMRowGAYIKoUDA4EDAQESDDAwNzcw
```

```
NzA0OTM4ODEYMBYGBSqFA2QBEg0xMDI3NzAwMTk4NzY3MSgwJgYDVQQKDB/Qn9CQ0J4gwqvQoNC+0YHRgtC
10LvQtdC60L7QvMK7MSYwJAYDVQQHDB3QodCw0L3QutGCLdCf0LXRgtC10YDQsdGD0YDQszEpMCcGA1UECA
wgNzgg0KHQsNC90LrRgi3Qn9C10YLQtdGA0LHRg9GA0LMxCzAJBgNVBAYTAlJVMSgwJgYDVQQDDB/Qn9CQ0
J4gwqvQoNC+0YHRgtC10LvQtdC60L7QvMK7MGMwHAYGKoUDAgITMBIGByqFAwICJAAGByqFAwICHgEDQwAE
QN9eHf5trruzGfhJPjeX9nlXFGtOI+U36xVVsGczNTz8kwwgnt6h0yGTkT296O9cmb/4ZnaUSbj4vvIMQAz
XejajggSDMIIEfzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPnxGNuqnYf86yewtnZ3KsHOW0GZMIIBiA
YDVR0jBIIBfzCCAXuAFD7vGT8PuXmw8eYpIaPkuZW5pe6QoYIBTqSCAUowggFGMRgwFgYFKoUDZAESDTEyM
zQ1Njc4OTAxMjMxGjAYBggqhQMDgQMBARIMMDAxMjM0NTY3ODkwMSkwJwYDVQQJDCDQodGD0YnQtdCy0YHQ
utC40Lkg0LLQsNC7INC0LiAyNjEXMBUGCSqGSIb3DQEJARYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRgwFgY
DVQQIDA83NyDQnNC+0YHQutCy0LAxFTATBgNVBAcMDNCc0L7RgdC60LLQsDEkMCIGA1UECgwb0J7QkNCeIN
Cg0L7RgdGC0LXQu9C10LrQvtC8MTAwLgYDVQQLDCfQo9C00L7RgdGC0L7QstC10YDRj9GO0YnQuNC5INGG0
LXQvdGC0YAxNDAyBgNVBAMMK9Ci0LXRgdGC0L7QstGL0Lkg0KPQpiDQoNCi0JogKNCg0KLQm9Cw0LHRgSmC
EQFyCwFWUAC5s+cRzzq+NHegMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDAnBgkrBgEEAYI3FQo
EGjAYMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMB0GA1UdIAQWMBQwCAYGKoUDZHEBMAgGBiqFA2RxAjArBg
NVHRAEJDAigA8yMDE5MDMwNDEzMDg0MFqBDzIwMjAwMzA0MTMwODQwWjCCATQGBSqFA2RwBIIBKTCCASUMK
yLQmtGA0LjQv9GC0L7Qn9GA0L4gQ1NQIiAo0LLQtdGA0YHQuNGPIDMuOSkMLCLQmtGA0LjQv9GC0L7Qn9GA
0L4g0KPQpiIgKNCy0LXRgNGB0LjQuCAyLjApDGPQodC10YDRgtC40YTQuNC60LDRgiDRgdC+0L7RgtCy0LX
RgtGB0YLQstC40Y8g0KTQodCRINCg0L7RgdGB0LjQuCDihJYg0KHQpC8xMjQtMjUzOSDQvtGCIDE1LjAxLj
IwMTUMY9Ch0LXRgNGC0LjRhNC40LrQsNGCINGB0L7QvtGC0LLQtdGC0YHRgtCy0LjRjyDQpNCh0JEg0KDQv
tGB0YHQuNC4IOKEliDQodCkLzEyOC0yODgxINC+0YIgMTIuMDQuMjAxNjA2BgUqhQNkbwQtDCsi0JrRgNC4
0L/RgtC+0J/RgNC+IENTUCIgKNCy0LXRgNGB0LjRjyAzLjkpMGUGA1UdHwReMFwwWqBYoFaGVGh0dHA6Ly9
jZXJ0ZW5yb2xsLnRlc3QuZ29zdXNsdWdpLnJ1L2NkcC8zZWVmMTkzZjBmYjk3OWIwZjFlNjI5MjFhM2U0Yj
k5NWI5YTVlZTkwLmNybDBXBggrBgEFBQcBAQRLMEkwRwYIKwYBBQUHMAKGO2h0dHA6Ly9jZXJ0ZW5yb2xsL
nRlc3QuZ29zdXNsdWdpLnJ1L2NkcC90ZXN0X2NhX3J0bGFiczIuY2VyMAgGBiqFAwICAwNBACD706a8WMDd
iFimYlNM7J6VNBgz4EoqSGhxWpn1iCIJysDDjGih66xC2PvWq7Cjz2uqWAIcFPEo6mMF6cINJ/8=</ds:X5
09Certificate></ds:X509Data></ds:KeyInfo></ds:Signature></ns2:SMEVSignature></ns2:S
endRequestResponse>
```


Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8

{"result":true,"message":"Подпись валидна"}
```

Прикладные ошибки:

Код ответа HTTP	Значение параметра «code»	Описание ошибки
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса

401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа
400	ADR-0102	Представлена невалидная XML
400	ADR-0103	Передан неверный тип XML на проверку подписи (разрешенный тип сообщения для СМЭВ)

2.2.6 Функция "Проверки состояния модулей Адаптера"

Данная функция рекомендуется к использованию системой мониторинга КА для контроля функционирования модулей Адаптера. Вызовы осуществляются в пределах контролируемой зоны КА. Методы возвращает текущее состояние работоспособности модуля, обеспечивающего процесс регистрации БО и модуля, обеспечивающего процесс удаленной идентификации.

Реализация:

Аспект реализации	Реализация
Транспортный протокол	HTTPS
Аутентификация вызывающей стороны	Authorization - обязательный заголовок в запросе. Имеет вид Authorization: Bearer токен_доступа. Токен доступа прописывается в конфигурации Адаптера и выдается ППО ИС КА.

Поддерживаемый метод HTTP запроса:

```
GET
```

Путь для проверки состояния модуля, обеспечивающего процесс регистрации БО (относительно базового URL):

```
/reg/check
```

Примечание:
Запрос выполняется к модулю inner-smev-service и, в дополнение к базовому URL, должен содержать порт и контекст данного сервиса: 8082/inner-smev-service/
Например: https://{{adapter_url}}:8082/inner-smev-service/api/v1/reg/check

Путь для проверки состояния модуля, обеспечивающего процесс удаленной идентификации (относительно базового URL):

```
/vrf/check
```

Заголовки запроса:

```
Authorization: Bearer {{token}},
```

где {{token}} - токен доступа системы мониторинга КА к API.

Пример запроса:

```
GET /api/v1/vrf/check HTTP/1.1
Authorization: Bearer FAEA055D4EE948CEA031ACE10ECDAE49
```

Функция возвращает ответ с HTTP-кодом, сигнализирующим о состоянии соответствующего модуля Адаптера. Пример ответа:

```
HTTP/1.1 200 OK
```

Возможные HTTP-коды ошибок модулей Адаптера и их значения

HTTP-код	Значение
200	Модуль Адаптера функционирует в штатном режиме работы.
203	Отказ при вызове одного или нескольких HSM при условии, что хотя бы один HSM работоспособен. Сервис регистрации БО или удаленной идентификации ограничено доступен, без отказоустойчивости.
500	Критичная ошибка. Отказ при вызове всех HSM, либо СУБД (только для функции "/vrf/check"). Сервис регистрации БО или удаленной идентификации недоступен.

2.2.7 Внутренний API биометрической верификации с использованием IdP, отличного от ЕСИА

Используется ИС КА для запуска процесса верификации пользователя с привязкой к ID УЗ IDP (не ЕСИА) в ЕБС.

2.2.7.1 Функция «Создание сессии биометрической верификации»

Метод Адаптера. Вызывается ИС КА для создания сессии верификации.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

v2/vrf/create

Вызов:

POST <host>:<port>/api/v2/vrf/create

Входные параметры:

Параметр	Тип данных	Обязательность	Описание
sid	UUID	да	Идентификатор сессии Адаптера. Данный идентификатор является уникальным. Идентификатор состоит из прописных английский букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12
result_uri	String	да	URL "API получения результата верификации ИС КА", на который Адаптер должен вернуть

			результат биометрической верификации (см. п. 2.2.7.3)
public_uri	String	да	URL ИС КА на который будет перенаправлен Пользователь после успешной верификации.
client	JSON Object	да	Данные о контрагенте
client.client_id	String	да	Мнемоника Потребителя БДн
client.idp	String	да	Мнемоника IdP
client.user_id	String	да	Идентификатор УЗ пользователя IdP
client.meta	JSON Object	нет	Дополнительные данные о контрагенте. К примеру - contract_id, service_type.
client.meta.contract_id	String	нет	Дополнительные данные о контрагенте.
client.meta. service_type	String	нет	Дополнительные данные о контрагенте.
metadata	JSON Object	да	Содержит перечень дополнительных данных. Проверка наполнения данного параметра находится вне рамок ТИБ. Проверка наполнения осуществляется на стороне ЕБС (см. Приложение №1)
bio_collecting_type	String	да	Требуемая мнемоника согласованной схемы сбора БО. (см. Приложение №4)

Пример запроса:

```
POST /servlets/api/v2/vrf/create HTTP/1.1
Host: t01adaptertib:9000
```

```
Content-Type: application/json
Authorization: Bearer SIGN
Cookie: JSESSIONID=5866F558047FD093AF6929B1D5E1E24D
Content-Length: 638

{
        "sid": "2f9ca570-ec12-470d-b6d8-1cd94fcaa528",
        "result_uri": "https://otib-tkur.ebsbio.tech/ttib_callback",
        "public_uri": "https://otib-tkur.ebsbio.tech/ttib_callback2",
        "client": {
            "client_id": "TTIB",
            "idp": "http://stub.ebsbio.tech/iss_tib",
            "user_id": "1000589841",
            "meta": {
                "contract_id": "51684869",
                "service_type": "vrf"
            }
        },
        "metadata": {
                "date": "1605038455271"},
        "bio_collecting_type": "face_with_passive_liveness_and_webinterface"
    }
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ИС КА		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
400	ADR-0200	Сессия уже существует
401	ADR-0203	Невалидный Authorization Bearer. И описание ошибки: • "В запросе отсутствует header с названием Authorization"; • "В запросе невалидный header с названием Authorization"

500	ADR-0205	Внутренняя ошибка при работе с базой данных
500	ADR-0206	Попытка перехода сессии пользователя в запрещенное состояние
400	ADR-0210	Ошибка при отправке запроса в ЕБС

2.2.7.2 Функция «Передача verify_token в Адаптер и возврат res_secret»

Метод Адаптера. Вызывается ИС КА для передачи verify_token в рамках процесса биометрической верификации (в случае если для верификации используется WEB-форма ИС КА). Результатом является получение специального ключа для результатов аутентификации.

Важно! Если съем БО производился с использованием веб-интерфейса ЕБС, то ЕБС осуществит перенаправление пользователя ИС КА в Адаптер, и реализация данного метода не потребуется. В случае же использования своей веб-формы, ИС КА необходимо реализовывать данный метод.

Поддерживаемый метод HTTP запроса:

GET

Путь относительно базового URL:

v2/vrf/result?verify_token={verify_token}&expired={expired}&sid={sid}

Вызов:

GET <host>:<port>/api/v2/vrf/result?verify_token={verify_token}&expired={expired}&sid={sid}

Входные данные

Параметр	Тип данных	Обязательность	Описание
sid	UUID	да	Идентификатор сессии Адаптера, максимальное количество 255 символов, данный идентификатор является уникальным.
verify_token	String	да	Контрольное значение (уникальный идентификатор, созданный ЕБС), необходимое для получения расширенного результата верификации после успешной верификации.
expired	Number	да	Время прекращения действия результата биометрической верификации пользователя в ЕБС, в миллисекундах с 1 января 1970 г. 00:00:00 GMT.

Успешный ответ:

В результате метода осуществляется перенаправление пользователя в ИС КА. В Location содержится res_secret.

Выходные параметры

Параметр	Тип данных	Обязательность	Описание
res_secret	String	Нет	Уникальный идентификатор. Присутствует только в случае успешного прохождения пользователем протокола проведения идентификации и аутентификации (генерируется на стороне Адаптера).

Пример запроса:

```
GET /servlets/api/v2/vrf/result?sid=2f9ca570-ec12-470d-b6d8-
1cd94fcaa525&expired=1701340648442&verify_token=512df7be-3379-4a14-8ed3-
a5b4ec28b71f HTTP/1.1
```

Пример ответа:

```
HTTP/1.1 302
Location: https://test.esu-vks.ru?res_secret=81ec6a78-26e5-438e-a6d4-1f15d91c9d7c
```

Прикладные ошибки

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ИС КА		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
400	ADR-0200	Сессия уже существует
401	ADR-0203	Невалидный Authorization Bearer. И описание ошибки: •"В запросе отсутствует header с названием Authorization"; •"В запросе невалидный header с названием Authorization"
500	ADR-0205	Внутренняя ошибка при работе с базой данных
500	ADR-0206	Попытка перехода сессии пользователя в запрещенное состояние
400	ADR-0210	Ошибка при отправке запроса в ЕБС

2.2.7.3 Функция «Передачи результатов биометрической верификации от Адаптера в ИС КА»

Метод ИС КА. Вызывается ИС КА для получения результатов верификации от Адаптера в ИС КА.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/api/result_uri

Вызов:

GET <host>:<port>/api/result_uri

Входные данные

Параметр	**Тип данных**	**Обязательность**	**Описание**

sid	UUID	да	Идентификатор сессии Адаптера. Идентификатор состоит из прописных английский букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12.
auth_result	Boolean	да	Результат процесса биометрической верификации с использованием ЕБС
res_secret	String	да	Генерируемый Адаптером идентификатор в случае успешной верификации. Данный параметр передается Пользователю ИС КА и ИС КА, необходимый для предъявления Пользователем в ИС КА.
В случае возникновения ошибки			
sid	UUID	да	Идентификатор сессии Адаптера. Идентификатор состоит из прописных английский букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12.
auth_result	Boolean	да	Результат процесса биометрической верификации с использованием ЕСИА и ЕБС
code	String	да	Код ошибки верификации. Передается в случае возникновения ошибки при верификации.
message	String	да	Описание ошибки. Передается в случае возникновения ошибки при верификации.

Описание параметров code и message:

Ошибка, полученная от ЕБС	**Код ответа HTTP**	**Значение параметра «code»**	**Описание (параметр «message»)**
	400	ADR-0001	Отсутствуют обязательные данные
	500	ADR-0000	Внутренняя ошибка API
	500	ADR-0205	Внутренняя ошибка при работе с базой данных
	400	ADR-0210	Ошибка при отправке запроса в ЕБС
Любая другая ошибка, которая не указана ниже в таблице	400	ADR-0212	Ошибка формата данных, полученных из ЕБС
400 - EBS-010302	400	EBS-010302	Идентификатор сессии не найден
401 - EBS-010303	401	EBS-010303	Время жизни сессии истекло

Пример запроса с успешной верификацией:

```
POST /api/result_uri HTTP/1.1
Content-Type: application/json
{
“sid”: “5b9dcd00-71a6-4293-ac6c-f367a2ebef7f”,
“res_secret”: “81ec6a78-26e5-438e-a6d4-1f15d91c9d7c”,
«extended_result»:»{Base64 JWT Token с расширенным результатом
идентификации}»
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
```

Прикладные ошибки

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки на стороне ИС КА (реализует ИС КА)		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	BNK-0000	Внутренняя ошибка ИС КА
400	BNK-0001	Запрос не содержит обязательного параметра
400	BNK-0002	Неверные параметры запроса
400	BNK-0003	Сессия с указанным sid не существует

2.2.8 Внутренний API биометрической идентификации Адаптера

Используется ИС КА для биометрической идентификации пользователя с использованием Адаптера.

2.2.8.1 Функция "Создание сессии биометрической идентификации"

Метод Адаптера. Вызывается ИС КА для создания сессии идентификации. Идентичен методу создания сессии биометрической верификации в п. 2.2.7.1.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

v2/vrf/create

Вызов:

POST <host>:<port>/api/v2/vrf/create

Входные параметры:

Параметр	**Тип данных**	**Обязательность**	**Описание**
sid	UUID	да	Идентификатор сессии Адаптера. Данный идентификатор является уникальным. Идентификатор состоит из прописных английский букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12
result_uri	String	да	URL "API получения

			результата биометрической идентификации ИС КА", на который Адаптер должен вернуть результат биометрической идентификации.
public_uri	String	да	URL для перенаправления Пользователя после успешной верификации.
client	JSON Object	да	Данные о контрагенте
client.client_id	String	да	Мнемоника Потребителя БДн
client.idp	String	да	Мнемоника IdP
client.user_id	String	да	Идентификатор УЗ пользователя IdP
client.meta	JSON Object	нет	Дополнительные данные о контрагенте. К примеру - contract_id, service_type.
client.meta.key	String	нет	Дополнительные данные о контрагенте.
client.meta.value	String	нет	Дополнительные данные о контрагенте.
metadata	JSON Object	да	Содержит перечень дополнительных данных. Проверка наполнения данного параметра находится вне рамок ТИБ. Проверка наполнения осуществляется на стороне ЕБС (см. Приложение №1)
bio_collecting_type	String	да	Требуемая мнемоника согласованной схемы сбора БО (см.

			Приложение №4)
external_transaction_id	String	нет	Идентификатор транзакции на стороне ИС. Обязателен для процесса идентификации, в других случаях не заполняется.

Пример запроса:

```
POST https://example.com/api/v2/vrf/create HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache

{
    "sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
    "result_uri": "https://test.esu-vks.ru/",
    "public_uri": "https://test.esu-vks.ru/",
    "client": {
        "client_id": "TEST_SYSTEM",
        "idp": "https://example.com/urn",
        "user_id": "1213142412",
        "meta": {
            "contract_id": "123241",
            "service_type": "vrf"
        }
    },
    "metadata": {
        "date": "1520467814933",
        "time_zone": "2018-03-30T17:30:09.453+0500"
    },
    "bio_collecting_type": "face_and_voice_only",
    "external_transaction_id": "3d744bf8-c51b-4a41-bdd1-e59c2c041f55"
 }
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ИС КА		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
400	ADR-0200	Сессия уже существует
401	ADR-0203	Невалидный Authorization Bearer. И описание ошибки: •"В запросе отсутствует header с названием Authorization"; •"В запросе невалидный header с названием Authorization"
500	ADR-0205	Внутренняя ошибка при работе с базой данных
500	ADR-0206	Попытка перехода сессии пользователя в запрещенное состояние
400	ADR-0210	Ошибка при отправке запроса в ЕБС

2.2.8.2 Функция «Передача verify_token в Адаптер и возврат res_secret»

Метод Адаптера. Вызывается ИС КА для передачи verify_token в рамках процесса биометрической идентификации (в случае если для идентификации используется WEB-форма ИС КА). Результатом является получение специального ключа для результатов аутентификации. Идентичен методу передачи verify_token в Адаптер и возврата res_secret биометрической верификации в п. 2.2.7.2.

Важно! Если съем БО производился с использованием веб-интерфейса ЕБС, то ЕБС осуществит перенаправление пользователя ИС КА в Адаптер, и реализация данного метода не потребуется. В случае же использования своей веб-формы, ИС КА необходимо реализовывать данный метод.

Поддерживаемый метод HTTP запроса:

GET

Путь относительно базового URL:

v2/vrf/result?verify_token={verify_token}&expired={expired}&sid={sid}

Вызов:

GET <host>:<port>/api/v2/vrf/result?verify_token={verify_token}&expired={expired}&sid={sid}

Входные данные

Параметр	Тип данных	Обязательность	Описание
sid	UUID	да	Идентификатор сессии Адаптера, максимальное количество 255 символов, данный идентификатор является уникальным.
verify_token	String	да	Контрольное значение (уникальный идентификатор, созданный ЕБС), необходимое для получения расширенного результата верификации после успешной верификации.

expired	Number	да	Время прекращения действия результата биометрической верификации пользователя в ЕБС, в миллисекундах с 1 января 1970 г. 00:00:00 GMT.

Успешный ответ:

В результате метода осуществляется перенаправление пользователя в ИС КА. В Location содержится res_secret.

Выходные параметры

Параметр	Тип данных	Обязательность	Описание
res_secret	String	Нет	Присутствует только в случае успешного прохождения пользователем протокола проведения идентификации и аутентификации

Пример запроса:

```
GET /servlets/api/v2/vrf/result?sid=2f9ca570-ec12-470d-b6d8-
1cd94fcaa525&expired=1701340648442&verify_token=512df7be-3379-4a14-8ed3-
a5b4ec28b71f HTTP/1.1
```

Пример ответа:

```
HTTP/1.1 302
Location: https://test.esu-vks.ru?res_secret=81ec6a78-26e5-438e-a6d4-1f15d91c9d7c
```

Прикладные ошибки

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ИС КА		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
400	ADR-0200	Сессия уже существует
401	ADR-0203	Невалидный Authorization Bearer. И описание ошибки: • "В запросе отсутствует header с названием Authorization"; • "В запросе невалидный header с названием Authorization"
500	ADR-0205	Внутренняя ошибка при работе с базой данных
500	ADR-0206	Попытка перехода сессии пользователя в запрещенное состояние
400	ADR-0210	Ошибка при отправке запроса в ЕБС

2.2.8.3 Функция "Передачи результатов идентификации от Адаптера в ИС КА"

Метод Адаптера. Вызывается ИС КА для получения результатов биометрической идентификации от Адаптера в ИС КА. Идентичен методу направления результатов биометрической верификации в п. 2.2.7.3.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/api/result_uri

Вызов:

GET <host>:<port>/api/result_uri

Входные данные

Параметр	Тип данных	Обязательность	Описание
sid	UUID	да	Идентификатор сессии Адаптера. Идентификатор состоит из прописных английский букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12.
auth_result	Boolean	да	Результат процесса биометрической идентификации с использованием ЕСИА и ЕБС
res_secret	String	да	Генерируемый Адаптером идентификатор в случае успешной идентификации. Данный параметр передается Пользователю ИС КА и ИС КА, необходимый для предъявления Пользователем в ИС КА для получения результатов биометрической идентификации от ИС КА.
В случае возникновения ошибки			
sid	UUID	да	Идентификатор сессии Адаптера. Идентификатор состоит из прописных английских букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12.
auth_result	Boolean	да	Результат процесса биометрической идентификации с использованием ЕСИА и ЕБС
code	String	да	Код ошибки. Передается в случае возникновения ошибки при биометрической идентификации.
message	String	да	Описание ошибки. Передается в случае возникновения ошибки при биометрической идентификации.

Описание параметров code и message:

Ошибка, полученная от ЕБС	Код ответа HTTP	Значение параметра «code»	Описание (параметр «message»)
	400	ADR-0001	Отсутствуют обязательные данные
	500	ADR-0000	Внутренняя ошибка API
	500	ADR-0205	Внутренняя ошибка при работе с базой данных
	400	ADR-0210	Ошибка при отправке запроса в ЕБС
Любая другая ошибка, которая не указана ниже в таблице	400	ADR-0212	Ошибка формата данных, полученных из ЕБС
400 - EBS-010302	400	EBS-010302	Идентификатор сессии не найден
401 - EBS-010303	401	EBS-010303	Время жизни сессии истекло

Пример запроса с успешной идентификацией:

```
POST /api/result_uri HTTP/1.1
Content-Type: application/json
{
"sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
"res_secret": "81ec6a78-26e5-438e-a6d4-1f15d91c9d7c",
"extended_result":"{Base64 JWT Token с расширенным результатом
идентификации}"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
```

Прикладные ошибки

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки на стороне ИС КА (реализует ИС КА)		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	BNK-0000	Внутренняя ошибка ИС КА
400	BNK-0001	Запрос не содержит обязательного параметра
400	BNK-0002	Неверные параметры запроса
400	BNK-0003	Сессия с указанным sid не существует

2.2.9 Внутренний API регистрации пользователя через API

Используется ИС КА для регистрации пользователя с предоставлением БО (импорт БО) или без предоставления БО (привязка УЗ).

2.2.9.1 Функция "Регистрация пользователя"

Метод Адаптера. Вызывается со стороны ИС КА для начала процесса регистрации УЗ Пользователя в ЕБС. Метод используется как для регистрации УЗ, так и для импорта БО. В зависимости от service_type, передаваемого в запросе (с БО или без БО), перечень обязательных полей будет разным.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

v2/registration

Вызов:

POST <host>:<port>/api/v2/registration

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
Часть multipart для передачи не биометрических данных			
service_type	string	да	Тип (мнемоника) услуги Возможны следующие варианты мнемоник услуги регистрации: 1. reg-without-bio (передается для регистрации без БО); 2. reg-bio (передается для регистрации с БО не более одного образца каждой модальности; 3. reg-bio-set (для регистрации с БО с передачей более одного образца БО каждой модальности)
quality_id	integer	нет (для регистрации без БО) да (для регистрации с БО)	Уровень качества сбора. Данный параметр принимает значение 1. Если регистрация производится без БО, параметр не требуется (отсутствует). Если регистрация производится с

			БО, параметр требуется (должен быть заполнен).
result_uri	String	да	URL «API получения результатов регистрации ИС КА», на который Адаптер должен вернуть результат регистрации.
sid	UUID	да	Уникальный идентификатор сессии. Идентификатор состоит из прописных английских букв и цифр (0-9, a-z) и тире в формате 8-4-4-4-12
datetime_tz	number	да	Дата регистрации (Формат Unix time stamp в секундах)
infosystem	JSON-object	да	Содержит информацию о ИС Контрагента, отправившей запрос
infosystem.system_id	string	да	Мнемоника ИС Контрагента
infosystem.contract_id	string	да	Идентификатор контракта
infosystem.ra_id	string	нет - для регистрации без БО да - для регистрации с БО	Идентификатор центра обслуживания в реестре поставщика идентификации IdP/идентификатор офиса (филиала) КА. Если регистрация производится без БО, параметр не требуется (отсутствует). Если регистрация производится с БО, параметр требуется (должен быть заполнен).
infosystem.employee_id	string	нет - для регистрации без БО да - для регистрации с БО	Сотрудник, осуществляющий регистрацию. Если регистрация производится без БО, параметр не требуется (отсутствует). Если регистрация производится с

			БО, параметр требуется (должен быть заполнен).
agree	JSON-object	нет – для регистрации без БО нет - для регистрации с БО	Содержит информацию о согласии. Данный массив является необязательным параметром. В случае его заполнения обязательному указанию подлежит только элемент массива agree.date_from.
agree.agreement_id	string	нет	Идентификатор записи данных согласия в ИС КА. Если согласие для ИС КА получает ЕБС, то заполняется идентификатор согласия в ЕБС
agree.date_from	number	да	Дата, с которой действует согласие (Формат Unix time stamp в секундах). Подлежит обязательному указанию только в случае заполнения массива agree
agree.date_to	number	нет	Дата, до которой действует согласие (Формат Unix time stamp в секундах)
person	JSON-object	да	Содержит информацию о пользователе
person.idp	string	да	Идентификатор (мнемоника) IdP
person.user_id	string	да	ID УЗ пользователя IdP
person.contact	JSON-object	нет	Контактные данные пользователя
person.contact.phone	string	нет	Телефон пользователя, указывается в формате +7XXXXXXXXXX, где X цифра от 0 до 9
person.contact.email	string	нет	Электронная почта пользователя
matching	array	нет	Содержит данные для

			мэтчинга.
matching.key	string	да	Описание передаваемых данных для мэтчинга. Может принимать значения: 1. «hash» - Хэш ПДн; 2. «ESIA» - IdP; 3. "SNILS" – СНИЛС ФЛ
matching.value	string	да	Значения данных для мэтчинга (Хэш ПДн, OID или СНИЛС ФЛ). Указываются без разделителей (пробелов, тире, символов и т.д.)
bio_collecting	array	нет	Содержит информацию о биометрических данных
bio_collecting.name	string	да	Наименование передаваемых БО (поле в multipart)
bio_collecting.modality	string	да	Мнемоники модальностей. Важно На данный момент реализованы следующие модальности: • photo- лицо; • sound- голос;
bio_collecting.bio_metadata	json-объект	нет	Дополнительные данные по БО (согласно спецификации видов метаданных поля BioMetadata (bio_metadata) в Приложении №3). Является обязательным параметром для биометрического образца модальности «voice» (голос)
meta	JSON-object	нет	Дополнительные метаданные (согласно Спецификации параметров meta в

			Приложении №2). ТИБ не осуществляет проверку наполнения данного параметра (какие параметры внутри). Проверка наполнения на стороне ЕБС.
metrics	JSON-object	нет	Дополнительные данные о метриках системы (см. Спецификацию метрик съема БО процесса саморегистрации в Приложении №3). ТИБ не осуществляет проверку наполнения данного параметра (какие параметры внутри). Проверка наполнения на стороне ЕБС. **Важно!** Метрики обязательны для регистрации пользователя с предоставлением БО.
Часть multipart для передачи биометрических данных			

bs<part>	Части multipart	нет	Содержат биометрические образцы для извлечения БКШ. <part> - порядковый номер БО.
			Заголовочные поля:
			• Content-Disposition: form-data
			• Content-Type:
			  ○ image/jpeg, image/png;
			  ○ audio/wav;
			• name="bs<part>";
			• filename="xxx.jpg"

Пример запроса с отправкой БО:

```
POST /api/v2/registration HTTP/1.1
Host: t01adaptertib01.tkur.ebsbio.tech:8096
Authorization: Bearer TTIB_SIGN
Cookie: JSESSIONID=5866F558047FD093AF6929B1D5E1E24D
Content-Length: 2559
```

```
Content-Type: multipart/form-data;
 boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data;
name="bs1"; filename="stub_photo_1.0.0.jpg"
Content-Type: <Content-Type header here>
(data)
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data;
 name="bs2"; filename="ddv.wav"
Content-Type: audio/wav
(data)
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="params"

{    "service_type": "reg-bio",
"quality_id": 1,
    "sid": "72635fc9-dcbd-47d9-b4b6-0330d0040e01",
    "result_uri": "https://otib-tkur.ebsbio.tech/ttib_callback",
    "datetime_tz": 1693287271,
    "infosystem": {
        "system_id": "TTIB",
        "contract_id": "51684869",
            "ra_id": "1231144134144",
    "employee_id": "15497894564564897"
    },
    "agree": {
        "agreement_id": "12392737476-agreeID",
        "date_from": 1589277386,
        "date_to": 1683868229
    },
    "person": {
        "idp": "IDP",
        "user_id": "11111",
        "contact": {
            "email": "sergejignatev320@gmail.com"
        }
```

```
},
"matching": [{
    "key":"ESIA",
    "value": "111111"
}],
  "metrics":
    {"consent_time_start": "2019-12-02 13:00:22.473",
    "consent_time_end": "2019-12-02 13:00:56.298",
    "photo_time_start_1": "2019-12-02 13:01:24.946",
    "photo_time_start_2": "2019-12-02 13:02:14.336",
    "photo_time_end_1": "2019-12-02 13:01:53.865",
    "photo_time_end_2": "2019-12-02 13:02:46.467",
    "sound_direct_time_start_1": "2019-12-02 13:03:12.984",
    "sound_direct_time_end_1": "2019-12-02 13:03:43.123",
    "sound_reverse_time_start_1": "2019-12-02 13:04:02.452",
    "sound_reverse_time_end_1": "2019-12-02 13:04:16.123",
    "sound_random_time_start_1": "2019-12-02 13:04:35.984",
    "sound_random_time_end_1": "2019-12-02 13:04:53.123",
    "sound_all_time_end_1": "2019-12-02 13:05:51.486"},
"bio_collecting": [{
        "name": "bs1",
        "modality": "photo"
    },
    {
        "name": "bs2",
        "modality": "sound",
        "bio_metadata": {
            "voice_1_start": "00.000",
            "voice_1_end": "07.523",
            "voice_1_desc": "digits_asc",
                   "voice_2_start": "07.523",
            "voice_2_end": "14.489",
            "voice_2_desc": "digits_desc",
                   "voice_3_start": "14.489",
            "voice_3_end": "26.427",
            "voice_3_desc": "digits_random"
        }
     }
```

```
    ]
}
------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

Пример ответа:

```
HTTP/1.1 202 Accepted
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ИС КА		
HTTP	**code**	**Описание («message»)**
500	ADR-0000	Внутренняя ошибка API
500	ADR-0000	Внутренняя ошибка ИС КА
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа
400	ADR-0200	Сессия уже существует

2.2.10 Внутренние API приостановки действия (деактивации) УЗ

Используется для отправки запросов на деактивацию УЗ/БКШ из ИС КА с прохождением через Адаптер в ЕБС.

2.2.10.1 Функция «Деактивация УЗ»

Метод Адаптера. Вызывается со стороны ИС КА для направления запроса на деактивацию УЗ в ЕБС.

Поддерживаемый метод HTTP запроса:

DELETE

Путь относительно базового URL:

v1/tib-deactivate-acc

Вызов:

DELETE <host>:<port>/api/v1/tib-deactivate-acc

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client	JSON Object	да	Данные о контрагенте
client.idp	String	да	URL (URI, сопоставляемый с Мнемоникой IdP, являющийся уникальным идентификатором стороны, генерирующей токен)

client.user_id	String	да	Идентификатор УЗ пользователя IdP
metadata	JSON Object	нет	Содержит перечень дополнительных данных. Проверка наполнения данного параметра находится вне рамок ТИБ. Проверка наполнения осуществляется на стороне ЕБС (см. Спецификацию дополнительных метаданных (meta) в Приложении №1)

Пример запроса:

```
DELETE /api/v1/tib-deactivate-acc HTTP/1.1
Host: t01adaptertib:8097
Content-Type: application/json
Authorization: Bearer 31c8d060-b589-445c-9c2f-872f4619f45e
Cookie: JSESSIONID=5866F558047FD093AF6929B1D5E1E24D
Content-Length: 112

{
    "client": {
        "idp": "http://stub.ebsbio.tech/iss_tib",
        "user_id": "1111"
    }
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от ЕБС			**Ошибки от Адаптера в ИС КА**		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**	**HTTP**	**Значение параметра «code»**	**Описание (параметр «message»)**
500	EBS-010001 EBS-010002	Внутренняя ошибка API	500	ADR-0000	Внутренняя ошибка API
400	EBS-010103	Запрос не содержит обязательного параметра	400	ADR-0001	Запрос не содержит обязательного параметра
400	EBS-010003	Неверные параметры запроса	400	ADR-0002	Неверные параметры запроса
400	EBS-010118	Пользователь уже деактивирован	400	ADR-0303	Пользователь уже деактивирован
400	EBS-010301	Пользователь не найден	400	ADR-0304	Пользователь не найден
401	EBS-010101	Ошибка проверки маркера доступа	401	ADR-0003	Недействительный токен доступа. Ошибка

401	EBS-010102	Ошибка проверки ЭП Провайдера идентификации			аутентификации вызывающей стороны (ИС КА) по токену доступа
401	EBS-010104	Маркер доступа просрочен			
403	EBS-02030	Отказано в доступе. Указанный провайдер идентификации отсутствует в системе			
403	EBS-02031	Отказано в доступе. Указанный провайдер идентификации заблокирован в системе			

2.2.10.2 Функция «Деактивация БКШ»

Метод Адаптера. Вызывается со стороны ИС КА для направления запроса на деактивацию ранее импортированных БКШ в ЕБС.

Поддерживаемый метод HTTP запроса:

DELETE

Путь относительно базового URL:

v1/tib-deactivate

Вызов:

DELETE <host>:<port>/api/v1/tib-deactivate

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client	JSON Object	да	Данные о контрагенте
client.idp	String	да	URL (URI, сопоставляемый с Мнемоникой IdP, являющийся уникальным идентификатором стороны, генерирующей токен)
client.user_id	String	да	Идентификатор УЗ пользователя IdP
metadata	JSON Object	нет	Содержит перечень дополнительных данных. Проверка наполнения данного параметра находится вне рамок ТИБ. Проверка наполнения осуществляется на стороне ЕБС.
trust_circle	string	да	Мнемоника круга доверия

Пример запроса:

```
DELETE /api/v1/tib-deactivate HTTP/1.1
Host: t01adaptertib:8097
Content-Type: application/json
Authorization: Bearer 31c8d060-b589-445c-9c2f-872f4619f45e
Cookie: JSESSIONID=5866F558047FD093AF6929B1D5E1E24D
Content-Length: 143
```

```
{
    "client": {
        "idp": "http://stub.ebsbio.tech/iss_tib",
        "user_id": "1111"
    },
    "trust_circle": "fz-115"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от ЕБС			**Ошибки от Адаптера в ИС КА**		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**	**HTTP**	**Значение параметра «code»**	**Описание (параметр «message»)**
500	EBS-010001 EBS-010002	Внутренняя ошибка API	500	ADR-0000	Внутренняя ошибка API
400	EBS-010103	Запрос не содержит обязательного параметра	400	ADR-0001	Запрос не содержит обязательного параметра
400	EBS-010003	Неверные параметры запроса	400	ADR-0002	Неверные параметры запроса
400	EBS-010118	Пользователь уже деактивирован	400	ADR-0303	Пользователь уже деактивирован
400	EBS-010301	Пользователь не найден	400	ADR-0304	Пользователь не найден
401	EBS-010101	Ошибка проверки маркера доступа	401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа
401	EBS-010102	Ошибка проверки ЭП Провайдера идентификации			
401	EBS-010104	Маркер доступа просрочен			
403	EBS-02030	Отказано в доступе. Указанный провайдер идентификации отсутствует в системе			
403	EBS-02031	Отказано в доступе. Указанный провайдер идентификации заблокирован в системе			

2.2.11 Внутренний API удаления и получения БШ

Методы используются для передачи в ИС КА от ЕБС запросов с БШ и запросов на удаление ранее полученных БШ.

2.2.11.1 Функция «Выгрузка БКШ»

Метод ИС КА. Вызывается со стороны Адаптера для выгрузки БШ, полученных из ЕБС, в хранилище ИС КА (метод получения/выгрузки БШ из ЕБС описан в Методических рекомендациях по использованию сервисов выгрузки векторов и импорту БО).

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

v1/tib-in

Вызов:

POST <host>:<port>/api/v1/tib-in

Входные параметры:

Заголовки запроса: Cookie: ebs.session=<transactionId>,

где transactionId - идентификатор сессии между Адаптером и ИС КА (sid из запроса на регистрацию, направленного от ИС КА в Адаптер – см. п. 2.2.9.1), при наличии.

Cookie не передается в случае отсутствия sid в БД Адаптера.

Служит для сопоставления с ранее отправленным запросом на регистрацию данных.

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
Часть multipart для передачи JSON			
params	Array [JSON-Object]	Да	Содержит **PAYLOAD (часть multipart с JWT)** целиком в неизменном виде, полученный от ЕБС Заголовочные поля: • Content-Disposition: form-data • Content-Type: application/json; • name="params";
Часть multipart для передачи БКШ			
<vendor-name>	Byte[]	Нет	Содержат биометрические шаблоны. <vendor-name> - Название вендора из vectors.vendor из json-object. Заголовочные поля: • Content-Disposition: form-data

			• Content-Type: application/octet-stream; • name="<vendor-name>"; • filename="<vendor-name>"; Данной части не будет, в случае отсутствия в ЕБС БШ, подходящих для ИС КА

Пример запроса:

```
POST /api/v1/tib-in
Cookie: ebs.session=5b9dcd00-71a6-4293-ac6c-f367a2ebef7f
Authorization: Bearer U29tZUJpb1NrdWRUb2tlbgo=
Type: multipart/form-data, Boundary: "bplwQXwyOEH2ve8r8lghSSrP_qKsi4N"
Content-Type: application/json\r\n
Content-Disposition: form-data; name="params"\r\n
Content-Length: 488\r\n\r\n
JavaScript Object Notation: application/json
aud:TEST-NEW
sub:446992
vectors:
      [{
            "bio_class": "import_high_class",
            "displayed_bio_type": "Стандартная",
            "expiration_date": 1770959294897,
            "modality": "photo",
            "signature": {
            "alg": "GOST3411_2012_256withGOST3410_2012_256",
            "data":
            "jpfVWl+T03yTC5bYw3kFFfygKE+lcmqljzAAsqN41KeAtpBkT8N0OaUtCKOGqR8eu3xfiV
            4Xa
            DfGSgfJQH3Hmg==",
            "keyId": "e3e2b851-b03f-4de0-939f-1ff341f22d2c",
            "type": "PLAIN"
            },
            "vendor": "stub_photo_1.0.0"
      }],
operation_type:uploading
exp:1676289119
iat:1676288519
Content-Type: application/octet-stream\r\n
```

```
Content-Disposition: form-data; name="stub_photo_1.0.0";
filename="stub_photo_1.0.0"\r\n
Content-Length: 4\r\n\r\n
Data (4 bytes)
Data: 48004900
```

Содержимое params:

```
{
          "sub": "extID1",
          "aud": "coffeebean",
          "operation_type": "uploading",
          "vectors": [
              {
                  "vendor": "IVACV_photo_1.2.1",
                  "modality": "photo",
                  "signature": {
                      "data":"Xjr7+EW7Qc7gxBWloH1RVHs5imTObCxZ+IC5w9poEH6ICH6boBvgz
      5aTSqpXoMQtLmemLeQqc8qT0glyfpM8kAo=",
                      "alg": "GOST3411_2012_256withGOST3410_2012_256",
                      "type": "PLAIN",
                      "keyId": "56ebbb7f-d67a-424d-8c52-41664ce872de"
                   }
              }
          ],
          "iat": 1643872206,
          "exp": 1644333905
      }
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ЕБС			**Ошибки на стороне ИС КА в Адаптер (реализует ИС КА)**		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**	**HTTP**	**Значение параметра «code»**	**Описание (параметр «message»)**
500	ADR-0000	Внутренняя ошибка API	500	BNK-0000	Внутренняя ошибка ИС КА

400	ADR-0001	Запрос не содержит обязательного параметра	400	BNK-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса	400	BNK-0002	Неверные параметры запроса
401	ADR-0203	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос	401	BNK-0004	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос

2.2.11.2 Функция «Удаление БКШ»

Метод ИС КА. Вызывается со стороны Адаптера для отправки запроса на удаление ранее выгруженного БШ от ЕБС в ИС КА (запрос со стороны ЕБС на удаление/деактивацию БШ в ИС КА описан в Методических рекомендациях по использованию сервисов выгрузки векторов и импорту БО).

Поддерживаемый метод HTTP запроса: POST

Путь относительно базового URL: v1/tib-delete

Вызов: POST <host>:<port>/api/v1/tib-delete

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
json_object	JSON-Object	да	Содержит **PAYLOAD (часть multipart с JWT)** целиком в неизменном виде, полученный от ЕБС в запросе внешнего API Удаление БКШ

Пример запроса:

```
POST /api/v1/tib-delete
Authorization: Bearer U29tZUJpb1NrdWRUb2tlbgo=
Content-Type: application/json
{
    "sub": "extID1",
    "aud": "coffeebean",
    "iat": 1643872206,
    "exp": 1644333905
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера в ЕБС			Ошибки на стороне ИС КА в Адаптер (реализует ИС КА)		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**	**HTTP**	**Значение параметра «code»**	**Описание (параметр «message»)**
500	ADR-0000	Внутренняя ошибка API	500	BNK-0000	Внутренняя ошибка ИС КА
400	ADR-0001	Запрос не содержит обязательного параметра	400	BNK-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса	400	BNK-0002	Неверные параметры запроса
401	ADR-0203	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос	401	BNK-0004	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос

2.2.12 Внутренние API информирования

Методы реализуются на стороне ИС КА, для получения запросов от Адаптера. Используется для информирования ИС КА с функцией Поставщика БДн и/или IdP о результатах регистрации, а также о результатах связывания учетных записей (учетные записи связаны в ЕБС) из ГИС ЕБС с прохождением запроса через Адаптер.

2.2.12.1 Функция "Информирование ИС КА с функцией Поставщика БДн о результате регистрации УЗ "

Метод ИС КА. Вызывается со стороны Адаптера для направления ответа с результатом регистрации УЗ после получения запроса из ЕБС.

Важно! Метод вызывается только в случае регистрации пользователя с БО.

Поддерживаемый метод HTTP запроса:

POST

URL запроса:

https://{tib producer registration results URL ИС КА}/,

где tib producer registration results URL ИС КА - адрес, по которому модуль Адаптер направляет ответ в ИС КА. Используется URL (result_uri) ИС КА, полученный от ИС КА в методе api/v2/registration (см. п. 2.2.9.1). Хранится в БД Адаптера.

Вызов:

POST https://{tib producer registration results URL ИС КА}/

Входные параметры:

Наименование параметра	Тип данных	Обязательность	Описание
json_object	JSON-	да	Тело запроса внешнего API Информирования

	Object		ИС КА с функцией Поставщика БДн о результатах регистрации УЗ, полученного от ЕБС (метод запроса описан в Методических рекомендациях по использованию сервисов выгрузки векторов и импорту БО)

Пример запроса:

```
POST https://exampleURL.ru/
Content-Type: application/json; charset=utf-8
Authorization:  Bearer tib_producer_registration_results_token


{
  "sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
  "status": 200,
  "bio_class": "import_high",
  "exp_on": 1795598795,
  "displayed_bio_type": "Стандартная"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки на стороне ИС КА (реализует ИС КА)		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	BNK-0000	Внутренняя ошибка ИС КА
400	BNK-0001	Запрос не содержит обязательного параметра
400	BNK-0002	Неверные параметры запроса
401	BNK-0004	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос

2.2.12.2 Функция " Информирование ИС КА с функцией IdP о результате регистрации УЗ "

Метод ИС КА. Вызывается со стороны Адаптера для направления уведомления с результатом регистрации УЗ после получения запроса из ЕБС.

Поддерживаемый метод HTTP запроса:

POST

URL запроса:

https://{tib idp registration results URL ИС КА}/,

где tib idp registration results URL ИС КА - адрес, по которому модуль Адаптер направляет ответ в ИС КА. URL ИС КА хранится в настройках конфигурации Адаптера.

Вызов:

POST https://{tib idp registration results URL ИС КА}/

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
json_object	JSON-Object	да	Тело запроса внешнего API Информирование ИС КА с функцией IdP о результатах регистрации УЗ, полученного от ЕБС (метод запроса описан в Методических рекомендациях по использованию сервисов выгрузки векторов и импорту БО)

Пример запроса:

```
POST https://exampleURL.ru/
Content-Type: application/json; charset=utf-8
Authorization:  Bearer tib_idp_registration_results_token


{
     "user_id": "989898235",
     "stu": "A",
     "bio_class":"import_high",
     "displayed_bio_type":"Подтвержденная",
     "exp_on":179559879
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки на стороне ИС КА (реализует ИС КА)		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	BNK-0000	Внутренняя ошибка ИС КА

400	BNK-0001	Запрос не содержит обязательного параметра
400	BNK-0002	Неверные параметры запроса
401	BNK-0004	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос

2.2.12.3 Функция "Информирование ИС КА с функцией IdP о результате связывания УЗ "

Метод ИС КА. Вызывается со стороны Адаптера для направления уведомления с результатом связывания УЗ после получения запроса из ЕБС.

Поддерживаемый метод HTTP запроса:

POST

URL запроса:

https://{tib idp matching result URL ИС КА},

где tib idp matching result URL ИС КА - адрес, по которому Адаптер направляет запрос с результатом мэтчинга в ИС КА с ролью провайдера идентификации (IDP). URL ИС КА берется из настроек конфигурации Адаптера.

Вызов:

POST https://{tib idp matching result URL ИС КА}/

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
json_object	JSON-Object	да	Тело запроса внешнего API Информирование ИС КА с функцией IdP о результатах связывания УЗ, полученного от ЕБС (метод запроса описан в Методических рекомендациях по использованию сервисов выгрузки векторов и импорту БО)

Пример запроса:

```
POST https://exampleURL.ru/
Content-Type: application/json; charset=utf-8
Authorization:  Bearer tib_registration_callback_wo_bo_token

{
    "sid": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
    "user_id": "1000453364",
    "stu": "MF"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки на стороне ИС КА (реализует ИС КА)		
HTTP	**Значение параметра «code»**	**Описание (параметр «message»)**
500	BNK-0000	Внутренняя ошибка ИС КА
400	BNK-0001	Запрос не содержит обязательного параметра
400	BNK-0002	Неверные параметры запроса
401	BNK-0004	Невалидный Authorization Bearer. Ошибка в случае невозможности авторизовать запрос

2.2.13 Внутренний API работы с согласиями в бумажном виде

Используется для отправки запросов с информацией о факте получения согласия клиента и/или отзыва согласия клиента на обработку персональных БДн в бумажном виде из ИС КА в ЕБС с прохождением запроса через Адаптер.

2.2.13.1 Функция «Отправка согласия»

Метод Адаптера. Вызывается со стороны ИС КА для отправки информации в ЕБС о факте дачи согласия клиента на обработку персональных БДн в бумажном виде в ИС КА.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

v1/permission/tib-issue

Вызов:

POST <host>:<port>/api/v1/permission/tib-issue

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client	JSON Object	да	Данные о контрагенте
client.iss	String	да	Чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, генерирующей токен (например https://test.idp.ru/urn)
client.idp	String	да	Мнемоника IdP
client.user_id	String	да	Идентификатор УЗ пользователя IdP
statement	String	Да	Человекочитаемый текст заявления организации, подтверждающий факт

			предоставления клиентом согласия на обработку БДн: *«Организация подтверждает, что клиент с приложенным ID предоставил согласие на обработку своих биометрических персональных данных.»*
ogrn	String	Да	ОГРН организации, получившей согласие пользователя
permission	JSON Object	Да	JSON-объект с параметрами согласия
permission.id	String	Нет	ID согласия на стороне организации, получившей согласие пользователя, либо другая дополнительная информация, облегчающая поиск согласия на стороне организации (кроме персональных данных)
permission.issued_on	Unix timestamp	Да	Дата и время начала действия согласия
permission.expired_on	Unix timestamp	Нет	Дата и время окончания действия согласия Не заполняется, если согласие бессрочное

Пример запроса:

```
POST /api/v1/permission/tib-issue HTTP/1.1
Host: t01adaptertib:8095
Content-Type: application/json
Authorization: Bearer df1f9f41-8367-4168-9c77-63e05bb9214e
Cookie: JSESSIONID=5866F558047FD093AF6929B1D5E1E24D
Content-Length: 428
{    "client": {
        "iss": "http://stub.ebsbio.tech/iss_tib",
        "idp":"TTIB-IDP",
        "user_id": "1000724604"
    },
   "statement":"Организация подтверждает, что клиент с приложенным ID предоставил
согласие на обработку своих биометрических персональных данных.",
   "ogrn":"1027700132195",
   "permission":{
      "id1":"32412313",
      "issued_on":"1665360000",
      "expired_on":"1791590400"}
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Ошибки метода:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа

2.2.13.2 Функция «Отзыв согласия»

Метод Адаптера. Вызывается со стороны ИС КА для отправки в ЕБС информации о факте отзыва согласия клиента на обработку персональных БДн в бумажном виде в ИС КА.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

v1/permission/tib-revoke

Вызов:

POST <host>:<port>/api/v1/permission/tib-revoke

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client	JSON Object	да	Данные о контрагенте
client.iss	String	да	Чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, генерирующей токен (например https://test.idp.ru/urn)
client.idp	String	да	Мнемоника IdP
client.user_id	String	да	Идентификатор УЗ пользователя IdP
statement	String	да	Человекочитаемый текст заявления организации, подтверждающий факт предоставления клиентом согласия на обработку БДн: *«Организация подтверждает, что клиент с приложенным ID произвел отзыв*

			согласия на обработку своих биометрических персональных данных.»
ogrn	String	Да	ОГРН организации, имеющей согласие пользователя
permission	JSON Object	Да	JSON-объект с параметрами согласия
permission.id	String	Нет	ID согласия на стороне организации, получившей согласие пользователя, либо другая дополнительная информация, облегчающая поиск согласия на стороне организации (кроме персональных данных)
permission.issued_on	Unix timestamp	Да	Дата и время отзыва согласия

Пример запроса:

```
POST /api/v1/permission/tib-revoke HTTP/1.1
Host: t01adaptertib:8095
Content-Type: application/json
Authorization: Bearer df1f9f41-8367-4168-9c77-63e05bb9214e
Cookie: JSESSIONID=5866F558047FD093AF6929B1D5E1E24D
Content-Length: 408
{
    "client": {
        "iss": "http://stub.ebsbio.tech/iss_tib",
        "idp": "TTIB-IDP",
        "user_id": "1000487659"
    },
   "statement":"Организация подтверждает, что клиент с приложенным ID произвел
отзыв согласия на обработку своих биометрических персональных данных.",
 "ogrn":"1027700132195",
   "permission":{
      "id":"32412313",
      "issued_on":"1669832378"
      }}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
500	ADR-0000	Внутренняя ошибка API
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА) по токену доступа

2.2.14 Внутренний API подписания и проверки подписи на ЕСИА-запросах

Используется ИС КА для подписания запроса на получение авторизационного кода ЕСИА, получение маркера доступа от ЕСИА для ИС КА и/или проверки подписи на токенах, пришедших от ЕСИА для ИС КА.

2.2.14.1 Функция «Подписание запроса на получение авторизационного кода ЕСИА» v1

Метод Адаптера. Вызывается со стороны ИС КА для подписания Адаптером запроса на получение авторизационного кода ЕСИА v1.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/adapter-esia/api/secret/ac/v1

Вызов:

POST <host>:<port>/adapter-esia/api/secret/ac/v1

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
scope	string	да	Область доступа, т.е. запрашиваемые права; например, если система- клиент запрашивает доступ к сведениям о сотрудниках организации, то scope должна иметь значение «http://esia.gosuslugi.ru/org_emps» (с необходимыми параметрами); если запрашивается scope id_doc68 (данные о пользователе), то не нужно в качестве параметра указывать oid этого пользователя
timestamp	datetime	да	Время запроса авторизационного кода в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>)

client_id	string	да	Идентификатор системы-клиента (мнемоника системы в ЕСИА указанная прописными буквами)
state	UUID	да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID

Выходные параметры в случае успешного ответа:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client_secret	string	да	Подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений четырех входящих параметров HTTP–запроса: scope, timestamp, client_id, state (без разделителей). Параметр <client_secret> должен быть закодирован в формате base64 url safe.

Пример запроса:

```
POST https://exampleURL.ru/adapter-esia/api/secret/ac/v1
Content-Type: application/json; charset=utf-8
Authorization:  Bearer U29tZUJpb1NrdWRUb2tlbgo=
{
      "scope": "openid",
      "timestamp": "2013.01.25 14:36:11 +0400",
      "client_id": "TESTAPPLICATION",
      "state": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
{
"client_secret": "xPufsnbiLsXN9X1JbAjkPLHS2nZL3-M7j-hAmNDA7GoL51JROKAuL0t9VE-
PUjN13RjCKGiodtGz02dUshlQKwHdjSIYj3XfzCZg_Rx8GGzlnsgd1P8RdJdvDKBJBL7_qhHNjHkf0yQ75S
eCaUvL0AR_UGNgp8Hr4e-sk7UoOWE"
}
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
400	ADR-0001	Запрос не содержит обязательного параметра

400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА по токену доступа
500	ADR-0000	Внутренняя ошибка API

2.2.14.2 Функция «Подписание запроса на получение авторизационного кода ЕСИА» v2

Метод Адаптера. Вызывается со стороны ИС КА для подписания Адаптером запроса на получение авторизационного кода ЕСИА v2.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/adapter-esia/api/secret/ac/v2

Вызов:

POST <host>:<port>/adapter-esia/api/secret/ac/v2

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client_id	string	да	Идентификатор системы-клиента (мнемоника системы в ЕСИА указанная прописными буквами)
scope	string	да	Область доступа, т.е. запрашиваемые права; например, если система- клиент запрашивает доступ к сведениям о сотрудниках организации, то scope должна иметь значение «http://esia.gosuslugi.ru/org_emps» (с необходимыми параметрами); если запрашивается scope id_doc68 (данные о пользователе), то не нужно в качестве параметра указывать oid этого пользователя
scope_org	string	нет	Область доступа, т.е. запрашиваемые права для юридических лиц; например, если система-клиент запрашивает доступ к сведениям об организации (hhtp://esia.gosuslugi.ru/org_inf), то не нужно в качестве параметра указывать oid организации этого пользователя.
timestamp	datetime	да	Время запроса авторизационного кода в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>)
state	UUID	да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса

			(необходимо для защиты от перехвата), генерируется по стандарту UUID
redirect_uri	string	да	Ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ к ресурсу. Значение <redirect_uri> должно быть предварительно указано в параметрах внешней ИС в ЕСИА – на стороне ЕСИА выполняется верификация соответствия redirect_uri в запросе и в настройках системы; Примечание: параметр не обязателен в рамках поддержки подписания запросов версии v1 API ЕСИА.

Выходные параметры в случае успешного ответа:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client_secret	string	да	Подпись запроса в формате ГОСТ Р 34.10-2012 с типом PLAIN в кодировке UTF-8 от значений шести входящих параметров HTTP–запроса: client_id, scope, scope_org, timestamp, state, redirect_uri. Параметр <client_secret> должен быть закодирован в формате base64 url safe.

Пример запроса:

```
POST https://exampleURL.ru/adapter-esia/api/secret/ac/v2
Content-Type: application/json; charset=utf-8
Authorization:  Bearer U29tZUJpb1NrdWRUb2tlbgo=
{
      "client_id": "TESTAPPLICATION",
      "scope": "openid",
      "scope_org": "org_inf",
      "timestamp": "2013.01.25 14:36:11 +0400",
      "state": "5b9dcd00-71a6-4293-ac6c-f367a2ebef7f",
      "redirect_uri": "https://test.application.ru/auth/api/v1/esia/return"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
{
"client_secret": "qaMf6UyZbCiAkCCgiexSh2Mmc_jGEVGK4KQSWBjdgfY8JNpU-
itPUQqXbcngr24a7mLY8b0_0FtmlzHs58AGmA"
}
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА по токену доступа
500	ADR-0000	Внутренняя ошибка API

2.2.14.3 Функция «Подписание запроса на получение маркера доступа ЕСИА» v1

Метод Адаптера. Вызывается со стороны ИС КА для подписания Адаптером запроса на получение маркера доступа ЕСИА v1.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/adapter-esia/api/secret/te/v1

Вызов:

POST <host>:<port>/adapter-esia/api/secret/te/v1

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
scope	string	да	Область доступа, т.е. запрашиваемые права (то же самое значение, которое было указано в запросе на получение авторизационного кода);
scope_org	string	Нет	Область доступа, т.е. запрашиваемые права для юридических лиц; например, если система-клиент запрашивает доступ к сведениям об организации (hhtp://esia.gosuslugi.ru/org_inf), то не нужно в качестве параметра указывать oid организации этого пользователя.
timestamp	datetime	да	Время запроса авторизационного кода в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>)
client_id	string	да	Идентификатор системы-клиента (мнемоника системы в ЕСИА указанная прописными буквами)

state	UUID	да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID; этот набор символов должен отличаться от того, который использовался при получении авторизационного кода;
redirect_uri	string	нет	Ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ (то же самое значение, которое было указано в запросе на получение авторизационного кода). Значение <redirect_uri> должно быть предварительно указано в параметрах внешней ИС в ЕСИА – на стороне ЕСИА выполняется верификация соответствия redirect_uri в запросе и в настройках системы; Примечание: параметр не обязателен в рамках поддержки подписания запросов версии v1 API ЕСИА.
code	string	да	Значение авторизационного кода, который был ранее получен от ЕСИА и который необходимо обменять на маркер доступа;

Выходные параметры в случае успешного ответа:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
client_secret	string	да	Подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений семи входящих параметров HTTP–запроса: scope, scope_org, timestamp, client_id, state (без разделителей), redirect_uri, code. Параметр <client_secret> должен быть закодирован в формате base64 url safe

Пример запроса:

```
POST https://exampleURL.ru/adapter-esia/api/secret/te/v1
Content-Type: application/json; charset=utf-8
Authorization:  Bearer U29tZUJpb1NrdWRUb2tlbgo=
{
      "scope": "openid",
      "scope_org": "org_inn",
      "timestamp": "2013.01.25 14:36:11 +0400",
      "client_id": "TESTAPPLICATION",
      "state": "d3b3f120-9ee5-4d2c-88b9-df9d84881867",
      "redirect_uri": "https://test.application.ru/auth/api/v1/esia/return"
      "code":"eyJ2ZXIiOjEsInR5cCI6IkpXVCIsInNidCI6ImF1dGhvcml6YXRpb25fY29kZSIsImFsZ
```

```
yI6IlJTMjU2In0.<...>.jGdT4nTEsUPBsnDOx3xx9EunRlSV8jmX6N4fCCnsbfABYAGB7aamTbcxBzFjIr
Egh_Ywopt250ICW8LZ55NWhbCiMWX4naySxypyMd3cwzdz_FP4VjUOj7US1SH9aGjxnYYENBOluCbPX7OPO
3OBKOQbxdXon
y-t1bWOi4mbGbMYTLsOxicoWzn2y1xDVpYrdoP-Rsry1ZOz1o4f8I9DV7i7_V08IuIti9OfXf5-
UlWPNdHNy2SllfyUthe6in9wbPuGaw_r92oC4BROVQkq7MpNX4hm-
PsUMRO6J4qM4hl3s_igPgh5TkC_NBNB0ySexgLhYEa_lifQCXPh-GkVbw2"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
{
    "client_secret": "xPufsnbiLsXN9X1JbAjkPLHS2nZL3-M7j-hAmNDA7GoL51JROKAuL0t9VE-
PUjN13RjCKGiodtGz02dUshlQKwHdjSIYj3XfzCZg_Rx8GGzlnsgd1P8RdJdvDKBJBL7_qhHNjHkf0yQ75S
eCaUvL0AR_UGNgp8Hr4e-sk7UoOWE"
}
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА по токену доступа
500	ADR-0000	Внутренняя ошибка API

2.2.14.4 Функция «Подписание запроса на получение маркера доступа ЕСИА» v3

Метод Адаптера. Вызывается со стороны ИС КА для подписания Адаптером запроса на получение маркера доступа ЕСИА v3.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/adapter-esia/api/secret/te/v3

Вызов:

POST <host>:<port>/adapter-esia/api/secret/te/v3

Входные параметры:

Наименование параметра	Тип данных	Обязательность	Описание
client_id	string	да	Идентификатор системы-клиента (мнемоника системы в ЕСИА, указанная прописными буквами)
scope	string	да	Область доступа, т.е. запрашиваемые права (то же самое значение, которое было указано в запросе на получение авторизационного кода);
scope_org	string	Нет	Область доступа, т.е. запрашиваемые права для юридических лиц; например, если система-клиент запрашивает доступ к сведениям об организации (hhtp://esia.gosuslugi.ru/org_inf), то не нужно в качестве параметра указывать oid организации этого пользователя.
timestamp	datetime	да	Время запроса авторизационного кода в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>)
state	UUID	да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID; этот набор символов должен отличаться от того, который использовался при получении авторизационного кода;
redirect_uri	string	нет	Ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ (то же самое значение, которое было указано в запросе на получение авторизационного кода). Значение <redirect_uri> должно быть предварительно указано в параметрах внешней ИС в ЕСИА – на стороне ЕСИА выполняется верификация соответствия redirect_uri в запросе и в настройках системы; Примечание: параметр не обязателен в рамках поддержки подписания запросов версии v1 API ЕСИА.
code	string	да	Значение авторизационного кода, который был ранее получен от ЕСИА и который необходимо обменять на маркер доступа;

Выходные параметры в случае успешного ответа:

Наименование параметра	Тип данных	Обязательность	Описание

client_secret	string	да	Подпись запроса в формате ГОСТ Р 34.10-2012 с типом PLAIN в кодировке UTF-8 от значений входящих параметров HTTP–запроса: client_id, scope, scope_org, timestamp, state, redirect_uri, code. Параметр <client_secret> должен быть закодирован в формате base64 url safe

Пример запроса:

```
POST https://exampleURL.ru/te-esia-signer
Content-Type: application/json; charset=utf-8
Authorization:  Bearer U29tZUJpb1NrdWRUb2tlbgo=
{
      "client_id": "TESTAPPLICATION",
      "scope": "openid",
      "scope_org": "org_inn",
      "timestamp": "2013.01.25 14:36:11 +0400",
      "state": "d3b3f120-9ee5-4d2c-88b9-df9d84881867",
      "redirect_uri": "https://test.application.ru/auth/api/v1/esia/return"
      "code":"eyJ2ZXIiOjEsInR5cCI6IkpXVCIsInNidCI6ImF1dGhvcml6YXRpb25fY29kZSIsImFsZ
yI6IlJTMjU2In0.<...>.jGdT4nTEsUPBsnDOx3xx9EunRlSV8jmX6N4fCCnsbfABYAGB7aamTbcxBzFjIr
Egh_Ywopt250ICW8LZ55NWhbCiMWX4naySxypyMd3cwzdz_FP4VjUOj7US1SH9aGjxnYYENBOluCbPX7OPO
3OBKOQbxdXon
y-t1bWOi4mbGbMYTLsOxicoWzn2y1xDVpYrdoP-Rsry1ZOz1o4f8I9DV7i7_V08IuIti9OfXf5-
UlWPNdHNy2SllfyUthe6in9wbPuGaw_r92oC4BROVQkq7MpNX4hm-
PsUMRO6J4qM4hl3s_igPgh5TkC_NBNB0ySexgLhYEa_lifQCXPh-GkVbw2"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8

{
    "client_secret": "qaMf6UyZbCiAkCCgiexSh2Mmc_jGEVGK4KQSWBjdgfY8JNpU-
itPUQqXbcngr24a7mLY8b0_0FtmlzHs58AGmA"
}
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
400	ADR-0001	Запрос не содержит обязательного параметра

400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА по токену доступа
500	ADR-0000	Внутренняя ошибка API

2.2.14.5 Функция «Проверки подписи на токенах, пришедших из ЕСИА»

Метод Адаптера. Вызывается со стороны ИС КА для проверки Адаптером подписи на токенах, пришедших от ЕСИА.

Поддерживаемый метод HTTP запроса:

POST

Путь относительно базового URL:

/adapter-esia/api/token/verification

Вызов:

POST <host>:<port>/adapter-esia/api/token/verification

Входные параметры:

Наименование параметра	**Тип данных**	**Обязательность**	**Описание**
esia_token	string	да	Токен, предоставленный ЕСИА в ответ на запрос на получение авторизацинного кода или маркера доступа

Выходные параметры в случае успешного ответа:

Параметр	**Тип данных**	**Обязательность**	**Описание**
result	Булево выражение	Да	Результат проверки ЭП
message	Строка	Нет	Описание результата

Пример запроса:

```
POST https://exampleURL.ru/adapter-esia/api/token/verification
Content-Type: application/json; charset=utf-8
Authorization:  Bearer U29tZUJpb1NrdWRUb2tlbgo=
{
    "esia_token":= "eyJ2ZXIiOjEsInR5cCI6IkpXVCIsInNidCI6ImF1dGhvcml6YXRpb25fY29kZSI
sImFsZyI6IlJTMjU2In0.<...>.jGdT4nTEsUPBsnDOx3xx9EunRlSV8jmX6N4fCCnsbfABYAGB7aamTbcx
BzFjIrEgh_Ywopt250ICW8LZ55NWhbCiMWX4naySxypyMd3cwzdz_FP4VjUOj7US1SH9aGjxnYYENBOluCb
PX7OPO3OBKOQbxdXon
y-t1bWOi4mbGbMYTLsOxicoWzn2y1xDVpYrdoP-Rsry1ZOz1o4f8I9DV7i7_V08IuIti9OfXf5-
UlWPNdHNy2SllfyUthe6in9wbPuGaw_r92oC4BROVQkq7MpNX4hm-
PsUMRO6J4qM4hl3s_igPgh5TkC_NBNB0ySexgLhYEa_lifQCXPh-GkVbw2"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json; charset=UTF-8
{
    "result": true,
    "message": "Подпись валидна"
}
```

Прикладные ошибки:

В случае возникновения ошибки при обработке запроса, вызывающей стороне возвращаются коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Ошибки от Адаптера		
HTTP	**code**	**Описание («message»)**
400	ADR-0001	Запрос не содержит обязательного параметра
400	ADR-0002	Неверные параметры запроса
401	ADR-0003	Недействительный токен доступа. Ошибка аутентификации вызывающей стороны (ИС КА по токену доступа
500	ADR-0000	Внутренняя ошибка API

2.3 Требования к поддерживаемым криптографическим алгоритмам

Адаптер реализует следующие криптографические функции, требуемые в рамках автоматизируемых процессов:

- формирование и проверка ЭП в соответствии с алгоритмами ГОСТ Р 34.10-2012 (256/512 бит) и ГОСТ 34.10-2018;
- вычисление значения хэш-функции в соответствии с алгоритмами ГОСТ Р 34.11-2012 (256/512 бит) и ГОСТ 34.10-2018.

Адаптер реализует следующие форматы ЭП, требуемые в рамках автоматизируемых процессов:

- ЭП в виде строки байт, кодированная в формате base64. Используется при подписании запросов и проверке ЭП ответов СМЭВ 3 при обращении к виду сведений, опубликованном на СМЭВ 3;
- PKCS#7 detached. Используется:
  - при подписании и проверке ЭП вложений (для формирования блока заголовков и ЭП вложений (//RefAttachmentHeaderList) сообщений СМЭВ3);
  - в процессе формирования ЭП запросов на авторизацию, получение маркеров доступа и обновления при взаимодействии с ЕСИА;
- JWT с CAdES-T. Используется в процессе проверки ЭП на токенах, полученных от ЕСИА, результатах верификации, полученных от ЕБС.

2.3.1 Требования к проверке ЭП в Адаптере

При проверке ЭП Адаптер проводит проверки действительности сертификатов:

- проверка ЭП сертификатов из цепочки сертификатов КА и сертификатов ГУЦ;
- проверка сроков действия сертификатов из цепочки сертификатов КА и сертификатов ГУЦ;
- проверка области использования сертификата КА для создания/проверки ЭП;
- проверка сертификатов из цепочки сертификатов пользователя на отозванность по СОС в соответствии с регламентом ГУЦ;
- проверка сроков действия СОС;
- проверка ЭП СОС;
- проверка наличия СОС.

2.4 Требования к эксплуатации

Эксплуатировать Адаптер необходимо с учетом требований, приведенных в документации на HSM, входящий в состав Адаптера.

2.5 Требования к численности, квалификации и функциям персонала Адаптера, режимам его работы

В функционировании Адаптера участвует эксплуатационный персонал:

- администраторы;
- администраторы информационной безопасности;

Основными обязанностями системного администратора являются:

- модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих станций);
- установка, модернизация, настройка и мониторинг работоспособности системного и общего программного обеспечения;
- установка, настройка и мониторинг программного обеспечения;
- ведение учетных записей пользователей Адаптера;
- контроль технического состояния оборудования;
- замена оборудования;
- обслуживание оборудования в соответствии с требованиями инструкций по эксплуатации этого оборудования фирм-производителей;
- обновление ПО;
- резервное копирование;

- работы по восстановлению данных из резервных копий;
- эксплуатация HSM;
- генерация ключевой информации в СКЗИ и установка сертификатов открытого ключа;
- удаление параметров Адаптера;
- удаление ключевой информации в СКЗИ.

Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств, применяемых в системе.

Основными обязанностями администраторов информационной безопасности являются:

- разработка, управление и реализация эффективной политики информационной безопасности Адаптера;
- управление правами доступа пользователей к функциям Адаптера;
- осуществление мониторинга информационной безопасности;
- анализ журналов событий.

Администратор информационной безопасности данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по обеспечению информационной безопасности.

Численность персонала должна быть установлена из расчета обеспечения работоспособности Адаптера во всех режимах функционирования.

Режим работы эксплуатационного персонала определяется режимом работы организации, эксплуатирующей Адаптер, за исключением работ по устранению возможных ошибок ПО, проводимых по регламенту в нерабочее время.

3 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

3.1 Требования к комплексу технических средств, его размещению на объекте

3.1.1 Требования к размещению комплекса технических средств в инфраструктуре КА

Размещение технических средств Адаптера необходимо проводить с учетом требований и инструкций по размещению технических средств, приведенных в документации на HSM и средств защиты информации, входящих в состав Адаптера.

3.1.2 Создание условий функционирования Адаптера

КА необходимо:

1. получить квалифицированный сертификат ключа проверки ЭП банка, созданного аккредитованным Минкомсвязью России удостоверяющим центром (ФГБУ НИИ «Восход») с применением средств удостоверяющего центра класса не ниже КВ2;
2. обеспечить подключение к ЕСИА, согласно регламентам и инструкциям для подключения к ЕСИА;
3. обеспечить подключение к СМЭВ 3, согласно регламентам и инструкциям для подключения к СМЭВ 3.х;
4. произвести пуско-наладочные работы КТС Адаптера в инфраструктуре КА, с учетом рекомендаций раздела **Ошибка! Источник ссылки не найден.**;
5. настроить Адаптер согласно руководству администратора;
6. обеспечить сетевые доступы для взаимодействий Адаптера со смежными Системами и пользователями;
7. обеспечить сетевые доступы от Адаптера до СОС и OCSP-служб, аккредитованных УЦ для проверки актуальности сертификатов ЭП;
8. настроить СЗИ КА:
    - средства межсетевого экранирования уровня приложений (WAF);
    - средства защиты от отказа в обслуживании (DDOS);
    - средства предотвращения вторжений (IPS);
    - создать подразделения и службы, необходимые для функционирования Адаптера.

4 ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Требования к техническим средствам защиты каналов взаимодействия

Сетевая схема взаимодействия технических средства защиты каналов взаимодействия приведена на рисунке ниже (см. **Ошибка! Источник ссылки не найден.**).

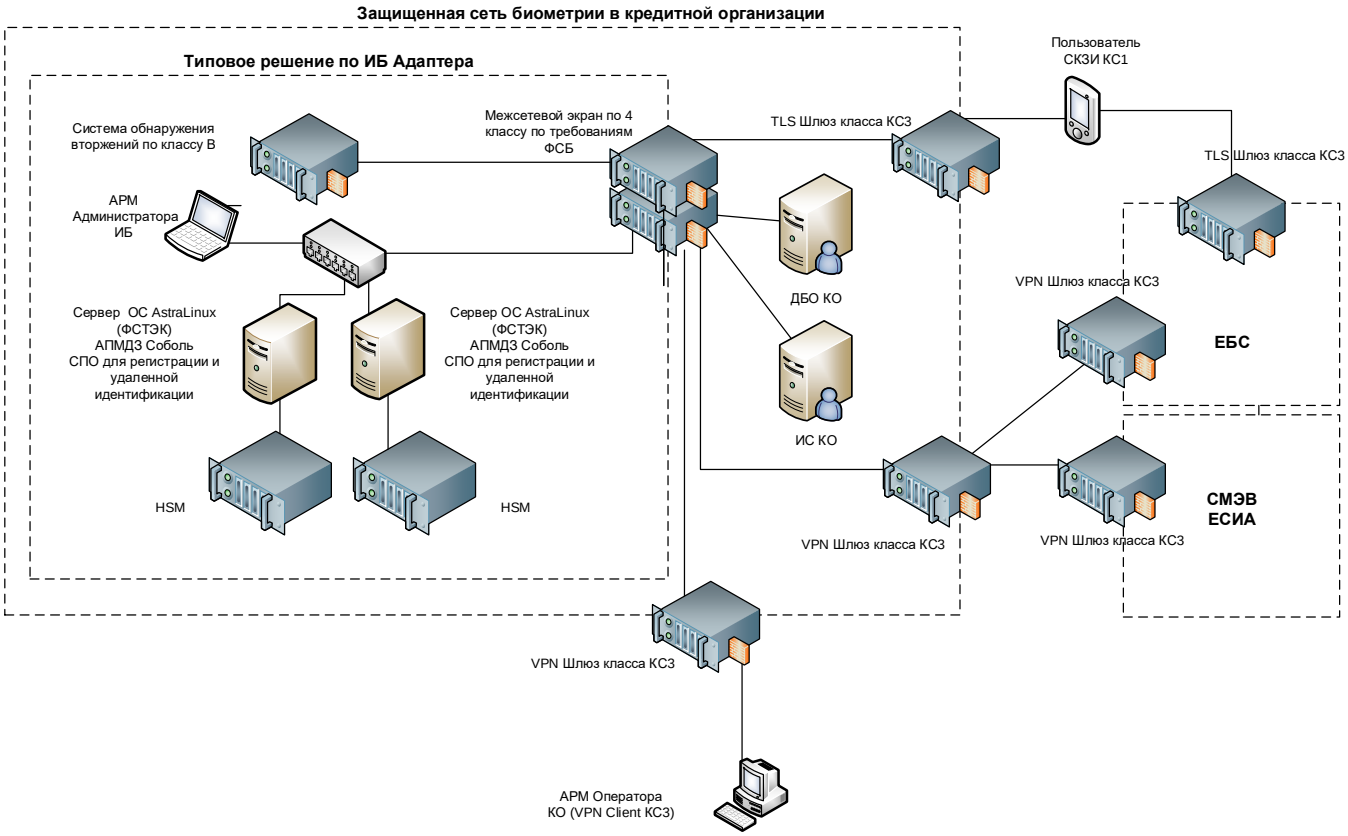


Рисунок 7 Схема взаимодействия технических средства защиты каналов взаимодействия

При реализации защиты персональных данных, передаваемых по каналам связи, должны применяться СКЗИ, сертифицированные по классу не ниже КС3 для каналов:

- между ИС КА и СМЭВ 3;
- между Адаптером и ЕСИА;
- между Адаптером и ЕБС.

При реализации защиты персональных данных, передаваемых по каналам связи между устройством пользователя (мобильным приложением ЕБС) и Адаптером:

- должны применяться СКЗИ на устройстве пользователя, сертифицированные по классу КС1;
- должны применяться СКЗИ на стороне Адаптера, сертифицированные по классу КС3.

Канал связи между устройством пользователя (мобильным приложением ЕБС) и Адаптером должен быть защищен с использованием протокола TLS с односторонней аутентификацией (аутентификация TLS-шлюза на стороне Адаптера). Реализация протокола TLS в TLS-шлюзе должна быть выполнена с учетом методических рекомендаций ТК 26 МР 26.2.001-2013 "Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)".

Если физическое лицо для удаленной идентификации с использованием ЕБС отказывается от применения шифровальных (криптографических) средств (в случаях, указанных в разделе **Ошибка! Источник ссылки не найден.**) СКЗИ не применяются.

В рамках протокола удаленной идентификации по открытому каналу между мобильным приложением банка и ИС КА передаются:

- запрос от пользователя к ИС КА на предоставление услуги, требующий аутентификации;
- ответ от ИС КА, содержащий перенаправление на Адаптер для прохождения удаленной аутентификации с указанием сгенерированного ИС КА идентификатору сессии.

В процессе встраивания данного решения в инфраструктуру банка необходимо обеспечить очистку идентификаторов сессии после предоставления услуги.

Все остальные взаимодействия в рамках протокола удаленной идентификации происходят либо в пределах контролируемой зоны, либо по защищенным соединениям. Подробные схемы взаимодействия в рамках протокола удаленной идентификации приведены в разделах **Ошибка! Источник ссылки не найден.** и **Ошибка! Источник ссылки не найден.**.

4.2 Требования к защите информации от несанкционированного доступа

При использовании Адаптера для защиты информации от несанкционированного доступа требуется:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего

персонала и посторонних лиц;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации Адаптера;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;
- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных средствами СЗИ КА;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности КА);
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации, и аутентификации пользователей;
- фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом);
- периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы средствами СЗИ КА;
- активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности средствами СЗИ КА;
- применение средств защиты информации, сертифицированных по системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, не ниже 3 класса, в том числе:
- средства (системы) защиты информации от несанкционированного доступа (далее – СЗИ от НСД);
- средства защиты информации от воздействия вредоносного кода (далее – СЗИ от ВВК);
- средства межсетевого экранирования;

- средства(системы) обнаружения вторжений (компьютерных атак).
- размещение объектов информационной инфраструктуры, используемых в Системе, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.
- КА для объектов информационной инфраструктуры Системы и ИС КА в пределах сегмента (группы сегментов) вычислительных сетей применять меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный ГОСТ Р 57580.1-2017.
- системно значимым кредитным организациям для объектов информационной инфраструктуры Адаптера и ИС КА в пределах сегмента (группы сегментов) вычислительных сетей, применять меры защиты информации, реализующие усиленный уровень (уровень 1) защиты информации, определенный ГОСТ Р 57580.1-2017.

ПРИЛОЖЕНИЕ №1. ДОПОЛНИТЕЛЬНЫЕ МЕТАДАННЫЕ (META)

Все параметры metadata, перечисленные в таблице ниже, имеют тип String.

Для сервиса биометрической верификации и сервиса биометрической идентификации обязательным для указания во всех запросах параметром является только параметр date, остальные можно не указывать.

Помимо целевого значения, все параметры, за исключением: date, могут принимать следующие значения:

- unknown – значение неизвестно;
- empty – значение пустое;
- error – возникла ошибка при получении значения;
- not_perm – нет разрешений на получения значения.

№	Наименование параметра	Обязательность	Описание	Формат	Пример
1.	date	Обязательное	Дата и время начала операции (формирования запроса клиентом)	timestamp	1520467814933
2.	time_zone	Обязательное	Временная зона: − Год; − Месяц; − День; − Часы; − Минуты; − Секунды; − временная зона	yyyy-MM-dd'T'HH:mm:ss.SSSZ	2018-03-30T17:30:09.453+0500
3.	geolocation	Обязательное	Координаты (Геолокация): широта и долгота	latitude;longitude	51.7556415;55.1028652
4.	rooted	Обязательное	Наличие jailbreak или root-доступа в операционной системе	true/false	true
5.	operating_system	Обязательное	Операционная система устройства: − название; − версия	name version	Android 6.0.1
6.	isp	Обязательное	Провайдер	name	MegaFon
7.	advertising_id	Обязательное	Идентификатор рекламы устройства (AdID в Android и IDFA в iOS)	value	38400000-8cf0-11bd-b23e-10b96e40000d
8.	screen	Обязательное	Разрешение экрана	width;height	1200;1920
9.	dpi	Обязательное	Плотность экрана устройства - значение, единицы измерения плотности пикселей	value	320 Dpi
10.	camera_id	Обязательное	Идентификатор камеры	name	2

11.	locale	Обязательное	Региональные настройки (локаль): страна, язык, название временной зоны. Данный параметр зависит от устройства и выбранных пользователем настроек.	country;language;timezonename	RU;ru;Москва, стандартное время
12.	device_serial	Обязательное	Серийный номер мобильного устройства.	deviceNumber	0819da27
13.	imei	Обязательное	IMEI - международный идентификатор мобильного оборудования	value	357719051789508
14.	device_id	Обязательное	Уникальный идентификатор Android-устройства	value	d1b23ев2f3b480cb
15.	device_manufacturer	Обязательное	Производитель устройства	name	asus
16.	device_model	Обязательное	Модель устройства	name	Nexus 7
17.	device_cpu	Обязательное	Информация о процессоре устройства	value	ARMv7 Processor rev 0 (v7l)
18.	sim	Обязательное	Информация о SIM-карте: − оператор; − название оператора; − страна; − номер сим карты. Можно отдавать раздельно.	simOperator;simOperatorName; simCountryIso;simSerialNumber	25002;MegaFon;ru;897210285241754519
19.	local_ip_address	Необязательное	Уникальный внутренний числовой идентификатор устройства в сети по протоколу IP	string	127.0.0.0

20.	ra_id	Необязательное		string	45938995
21.	employee_id	Необязательное	Идентификатор работника	string	2393288939302
22.	manufacturer	Необязательное	Сведения о производителе	string	789

ПРИЛОЖЕНИЕ №2. ДОПОЛНИТЕЛЬНЫЕ ДАННЫЕ О МЕТРИКАХ СИСТЕМЫ (METRICS)

Формат данных:

- дата и время события в формате YYYY-MM-DD HH:MM:SS.MsMsMs;
- string – строка, не пустая;

Помимо целевого значения, все параметры в зависимости от процесса регистрации могут принимать следующие значения:

- unknown – значение неизвестно;
- empty – значение пустое;
- error – возникла ошибка при получении значения;
- not_perm – нет разрешений на получение значения.

Набор обязательных параметров (проверяются в запросе) является исчерпывающим. Набор необязательных параметров (не проверяются в запросе) является неограниченным.

№	Мнемоника	Тип данных	Обязательность	Описание
1.	total_reg_time_end	timestamp	Обязательное	Время завершения процесса подготовки пакета и готовности направить пакет в ЕБС
2.	new_client_time_start	timestamp	Необязательное	Событие при входе в бизнес-процесс создания нового Клиента в системе поставщика БО или регистрирующего партнера, в случае если Клиент не был найден и его создание необходимо для старта процесса сбора
3.	new_client_time_end	timestamp	Необязательное	Событие перехода к процессу регистрации на стороне поставщика БО или регистрирующего партнера после создания нового Клиента в системе постащика БО или регистрирующего партнера.

4.	consent_time_start	timestamp	Необязательное	Событие процесса регистрации, которое инициализует сбор согласия на передачу БПДн (вывод экранной формы, запрос такого вывода с Бэк приложения, печать согласия и иное)
5.	consent_time_end	timestamp	Необязательное	Событие процесса регистрации, при котором клиентом было выражено согласие на передачу БПДн (акцепт, переход на экранную форму, отметка оператора и иное) При отсутствии возможности определения timestamp события, передавать <Value>2000-01-01 00:00:00.000</Value>
6.	photo_time_start_<part>	timestamp	Обязательное	Дата и время, когда инициировано на стороне сервера или прикладного ПО начало съемки лица клиента. Для каждой попытки, последовательно.
7.	photo_time_end_<part>	timestamp	Обязательное	Дата и время завершения сбора БО изображения лица (получение изображения сервером). Для каждой попытки, последовательно
8.	front_bqc_estimators_photo_<part>	string	Обязательное	Строка, передаваемая с библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества БО изображения лица. Для каждой попытки, последовательно.
9.	sound_direct_time_start_<part>	timestam	Обязательное	Дата и время, когда

		p	(при съеме БО) / необязательное (если не снимается БО)	инициировано на стороне сервера или прикладного ПО начало сбора первого БО записи голоса. Для каждой попытки, последовательно.
10.	sound_direct_time_end_<part>	timestamp	Обязательное (при съеме БО) / необязательное (если не снимается БО)	Дата и время завершения сбора первого БО записи голоса (получение записи сервером). Для каждой попытки, последовательно.
11.	front_bqc_estimators_sound_direct_<part>	string	Обязательное (при съеме БО) / необязательное (если не снимается БО	Строка, передаваемая с библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества первого БО записи голоса. Для каждой попытки, последовательно
12.	sound_reverse_time_start_<part>	timestamp	Обязательное (при съеме БО) / необязательное (если не снимается БО)	Дата и время, когда инициировано на стороне сервера или прикладного ПО начало сбора второго БО записи голоса. Для каждой попытки, последовательно.
13.	sound_reverse_time_end_<part>	timestamp	Обязательное (при съеме БО) / необязательное (если не снимается БО)	Дата и время завершения сбора второго БО записи голоса (получение записи сервером). Для каждой попытки, последовательно.
14.	front_bqc_estimators_sound_reverse_<part>	string	Обязательное (при съеме БО) / необязательное (если не снимается БО	Строка, передаваемая с библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества второго БО записи голоса. Для каждой попытки, последовательно
15.	sound_random_time_start_<part>	timestam	Обязательное	Дата и время, когда

		p	(при съеме БО) / необязательное (если не снимается БО)	инициировано на стороне сервера или прикладного ПО начало сбора третьего БО записи голоса. Для каждой попытки, последовательно.
16.	sound_random_time_end_<part>	timestamp	Обязательное (при съеме БО) / необязательное (если не снимается БО)	Дата и время завершения сбора третьего БО записи голоса (получение записи сервером). Для каждой попытки, последовательно.
17.	front_bqc_estimators_sound_random_<part>	string	Обязательное (при съеме БО) / необязательное (если не снимается БО	Строка, передаваемая с библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества третьего БО записи голоса. Для каждой попытки, последовательно
18.	sound_all_time_end_<part>	timestamp	Обязательное (при съеме БО) / необязательное (если не снимается БО	Дата и время завершения проверки записи, склеенной в одну запись, на соответствие требованиям с использованием ПО или сервиса контроля качества. Для каждой попытки, последовательно
19.	front_bqc_estimators_sound_all_<part>	string	Обязательное (при съеме БО) / необязательное (если не снимается БО	Строка, передаваемая с библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества записи, склееной в одну запись. Для каждой попытки, последовательно
20.	bank_find_profile_time_start_<part>	timestamp	Обязательное (для АРМ) / необязательное	**Только для АРМ или сбора оператором**. Дата и время, когда уполномоченный

				сотрудник поставщика БО или или регистрирующего партнера инициировал отправку запроса по поиску учётной записи клиента в ЕСИА. Для каждой попытки
21.	bank_find_profile_time_end_<part>	timestamp	Обязательное (для АРМ) / необязательное	**Только для АРМ или сбора оператором**. Дата и время, когда ИС поставщика БО или регистрирующего партнера подтвердила приём сообщения от СМЭВ, содержащего ответ на запрос по поиску учётной записи в ЕСИА. Для каждой попытки
22.	esia_find_account_msg_id	string	Обязательное (для АРМ) / необязательное	**Только для АРМ или сбора оператором**. Идентификатор запроса на поиск УЗ в ЕСИА
23.	esia_confirm_msg_id	string	Обязательное (для АРМ) / необязательное	**Только для АРМ или сбора оператором**. Идентификатор запроса, направленного на подтверждение личности клиента, УЗ которого находится в одном из статусов: • упрощенная, готовая к подтверждению; • стандартная; • подтвержденная через ФГУП «Почта России»
24.	esia_register_by_simplified_msg_id	string	Обязательное (для АРМ) / необязательное	**Только для АРМ или сбора оператором**. Идентификатор запроса, направленного на подтверждение УЗ клиента КА в ЕСИА, имеющей статус «Упрощенная»

25.	esia_recover_msg_id	string	Обязательное (для АРМ) / необязательное	**Только для АРМ или сбора оператором**. Идентификатор запроса обновления УЗ клиента в ЕСИА
26.	name_equipment_camera	string	необязательное	**В случае доступности такой информации.** Наименование оборудования (камера), если информация не доступна, не указывается
27.	name_equipment_microphone	string	необязательное	Наименование оборудования (микрофон)

ПРИЛОЖЕНИЕ №3. ВИДЫ МЕТАДАННЫХ ПОЛЯ

№	Key	Value	Описание	Примечание
1	voice_<part>_start	ss.SSS	Время начала записи голоса биом.образца от начала файла. ss – секунды, SSS - миллисекунды	Является обязательным атрибутом заполнения для биометрического образца модальности голос.
2	voice_<part>_end	ss.SSS	Время конца записи голоса биом.образца от начала файла. ss – секунды, SSS - миллисекунды	Является обязательным атрибутом заполнения для биометрического образца модальности голос.
3	voice_<part>_desc	digits_asc	На записи произнесены цифры в возрастающем порядке	Является обязательным атрибутом заполнения для биометрического образца модальности голос.
		digits_desc	На записи произнесены цифры в убывающем порядке	
		digits_random	На записи произнесены цифры в случайном порядке	
		text	На записи произнесен текст	

ПРИЛОЖЕНИЕ №4. ДОСТУПНЫЕ МНЕМОНИКИ СБОРА БО В ПРОЦЕССЕ БИОМЕТРИЧЕСКОЙ ВЕРИФИКАЦИИ

Мнемоника схемы сбора БО	Модальность		Необходимость инструкций проверки liveness (Active)	Необходимость проверки liveness (Passive)	Тип (URL) сбора на WEB интерфейсе		Content-Type (bio_sample)			Методы, используемые в процессе биометрической верификации в зависимости от мнемоники схемы сбора БО			
	Face	**Voice**			WEB интерфейс **не ЕБС**	WEB интерфейс **ЕБС**	**image/jpeg image/png multipart name= bs_photo**	**audio/wav multipart name= bs_audio**	**video/mp4 video/mov multipart name= bs_video**	**start**	**negotiate**	**upload**	**result**
FZ_115	1	1	1	0	0	1	0	0	1	1	1	1	1
face_only	1	0	0	0	1	0	1	0	0	1	0	1	1
voice_only	0	1	0	0	1	0	0	1	0	1	0	1	1
face_only_with_webinterface	1	0	0	0	0	1	1	0	0	1	0	1	1
voice_only_with_webinterface	0	1	0	0	0	1	0	1	0	1	0	1	1
face_with_passive_liveness	1	0	0	1	1	0	1	0	0	1	0	1	1
voice_with_passive_liveness	0	1	0	1	1	0	0	1	0	1	0	1	1
face_with_passive_liveness_and_webinterface	1	0	0	1	0	1	1	0	0	1	0	1	1
voice_with_passive_liveness_and_webinterface	0	1	0	1	0	1	0	1	0	1	0	1	1
face_with_active_liveness	1	0	1	0	1	0	0	0	1	1	1	1	1
voice_with_active_liveness	0	1	1	0	1	0	0	0	1	1	1	1	1
face_with_active_liveness_and_webinterface	1	0	1	0	0	1	0	0	1	1	1	1	1
voice_with_active_liveness_and_webinterface	0	1	1	0	0	1	0	0	1	1	1	1	1
face_with_all_liveness	1	0	1	1	1	0	0	0	1	1	1	1	1
voice_with_all_liveness	0	1	1	1	1	0	0	0	1	1	1	1	1
face_with_all_liveness_and_webinterface	1	0	1	1	0	1	0	0	1	1	1	1	1
voice_with_all_liveness_and_webinterface	0	1	1	1	0	1	0	0	1	1	1	1	1
face_and_voice_only	1	1	0	0	1	0	1	1	0	1	0	1	1

Мнемоника схемы сбора БО	Модальность		Необходимость инструкций проверки liveness (Active)	Необходимость проверки liveness (Passive)	Тип (URL) сбора на WEB интерфейсе		Content-Type (bio_sample)			Методы, используемые в процессе биометрической верификации в зависимости от мнемоники схемы сбора БО			
	Face	**Voice**			WEB интерфейс **не ЕБС**	WEB интерфейс **ЕБС**	**image/jpeg image/png multipart name= bs_photo**	**audio/wav multipart name= bs_audio**	**video/mp4 video/mov multipart name= bs_video**	**start**	**negotiate**	**upload**	**result**
face_and_voice_only_with_webinterface	1	1	0	0	0	1	1	1	0	1	0	1	1
face_and_voice_with_passive_liveness	1	1	0	1	1	0	1	1	0	1	0	1	1
face_and_voice_with_passive_liveness_and_webinterface	1	1	0	1	0	1	1	1	0	1	0	1	1
face_and_voice_with_active_liveness	1	1	1	0	1	0	0	0	1	1	1	1	1
face_and_voice_with_active_liveness_and_webinterface	1	1	1	0	0	1	0	0	1	1	1	1	1
face_and_voice_with_all_liveness	1	1	1	1	1	0	0	0	1	1	1	1	1
face_and_voice_with_all_liveness_and_webinterface	1	1	1	1	0	1	0	0	1	1	1	1	1

ПРИЛОЖЕНИЕ №5. ДОСТУПНЫЕ МНЕМОНИКИ СБОРА БО В ПРОЦЕССЕ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Мнемоника схемы сбора БО	Модальность		Необходимость инструкций проверки liveness (Active)	Необходимость проверки liveness (Passive)	Тип (URL) сбора на WEB интерфейсе		Content-Type (bio_sample)			Методы, используемые в процессе биометрической идентификации в зависимости от мнемоники схемы сбора БО			
	Face	**Voice**			WEB интерфейс **не ЕБС**	WEB интерфейс **ЕБС**	**image/jpeg image/png multipart name= bs_photo**	**audio/wav multipart name= bs_audio**	**video/mp4 video/mov multipart name= bs_video**	**start**	**negotiate**	**upload**	**result**
face_only	1	0	0	0	1	0	1	0	0	1	0	1	1
voice_only	0	1	0	0	1	0	0	1	0	1	0	1	1
face_only_with_webinterface	1	0	0	0	0	1	1	0	0	1	0	1	1
voice_only_with_webinterface	0	1	0	0	0	1	0	1	0	1	0	1	1
face_with_passive_liveness	1	0	0	1	1	0	1	0	0	1	0	1	1
voice_with_passive_liveness	0	1	0	1	1	0	0	1	0	1	0	1	1
face_with_passive_liveness_and_webinterface	1	0	0	1	0	1	1	0	0	1	0	1	1
voice_with_passive_liveness_and_webinterface	0	1	0	1	0	1	0	1	0	1	0	1	1
face_and_voice_only	1	1	0	0	1	0	1	1	0	1	0	1	1
face_and_voice_only_with_webinterface	1	1	0	0	0	1	1	1	0	1	0	1	1
face_and_voice_with_passive_liveness	1	1	0	1	1	0	1	1	0	1	0	1	1
face_and_voice_with_passive_liveness_and_webinterface	1	1	0	1	0	1	1	1	0	1	0	1	1