ИНФРАСТРУКТУРА БИОМЕТРИЧЕСКОЙ ПЛАТФОРМЫ

ЕДИНАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА

Методические рекомендации по работе

с Единой биометрической системой

Версия 1.16

Москва 2019

История документа

Версия	Дата	Автор	Комментарии
1.16	17.06.2019	Зиятдинов Р.Ф.	1. Добавление раздела 4.1.4.1, 5.1.1 и 5.2.1; 2. Корректировка разделов 5.1, 5.2; 3. Добавление раздела 2 Приложения Г «Руководство пользователя по работе с библиотекой ЕБС.Sdk»; 4. Корректировка разделов Приложения Г «Руководство пользователя по работе с библиотекой ЕБС.Sdk»; 5. Корректировка Приложения А Вид сведений в единой системе межведомственного электронного взаимодействия «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию»; 6. Добавление Приложений Д и Е;
1.15	10.04.2019	Курочкин В.С.	1. Скорректированы примеры в п.4.1.3.2.1; 2. Скорректировано описание в п.4.2.1; 3. Скорректировано описание п.4.2.2; 4. Скорректировано описание действий при ошибках верификации с использованием WEB-формы и МП ЕБС; 5. Обновлены ссылки на дистрибутив БКК и SDK.ЕБС; 6. Добавлено ПРИЛОЖЕНИЕ Г «Руководство пользователя по работе с SDK.ЕБС»
1.14	18.03.2018	Шульженко С.Н.	1. Скорректирован раздел 3.1; 2. В приложении Б скорректировано описание токена в п 5.3.2 и п 6.3.2; 3. Скорректирована схема процесса биометрической регистрации на Рисунке 1. 4. Удален раздел 4.2.2.2
1.13	18.12.2018	Курочкин В.С.	1. Скорректированы Таблица 2 и Рисунок 2 с описанием процесса удаленной идентификации с использованием МП раздел 3.2 2. Изменены адреса точки доступа к API биометрической верификации в разделе 2 Приложения Б; 3. Скорректировано описание VerifyToken, содержащегося в accessToken, полученного на этапе 2. Раздел 4.2.1.
1.12	23/08/2018	Шульженко С.Н.	1. Удалён раздел «Рекомендуемые условия для получения биометрических образцов в офисе кредитной организации; 2. В разделе 4.2.1 Указано, что после проведения биометрической верификации, ИС Потребителя БДн должна возвращать пользователя на WEB-форму или МП Потребителя БДн, с которых инициировался процесс; 3. По тексту изменен передаваемый в ИС Потребителя БДн результат. Результатом являются вероятности ошибки ложного совпадения по каждой модальности и общая; 4. Добавлена версия API «v2». 5. Скорректированы диаграммы на Рисунках 13 и 14; 6. Скорректированы разделы 5.3 и 6.3 ПРИЛОЖЕНИЯ Б; 7. Скорректирован раздел 7 ПРИЛОЖЕНИЯ Б;

			8. Скорректированы схемы Рисунок 2 и Рисунок 3;
1.11	09/08/2018	Курочкин В.С.	1. Скорректирован р. 4.2.1 (Этап 3); 2. Скорректирован р. 4.2.2.2; 3. Добавлен р. 5.2 Приложения Б; 4. Скорректировано Приложение В; 5. Добавлен параметр ответа в р. 5.1 Приложения Б; 6. Скорректировано описание алгоритма шифрования в р. 5.3 Приложения Б.
1.10	03/07/2018	Шульженко С.Н.	1. Удалены разделы 5.1 (метод «Получение конфигурации API ЕБС»), 5.3 (метод «Согласование методов сбора БО и Liveness») и 5.4 (метод «Приём БО на верификацию») Приложения Б; 2. Добавлен раздел 6 «Точка Доступа к ЕСИА» в Приложение Б; 3. В разделе 2 «Точка доступа к API биометрической верификации» Приложения Б добавлены адреса продуктивной среды ЕБС; 4. Скорректировано описание Успешного ответа метода «Старт верификации в ЕБС» в Приложении Б.
1.9	02/07/2018	Шульженко С.Н.	1. Раздел 4.2.1 Добавлено описание параметров, которые можно получить со scope «ext_auth_result»; 2. Приложение Б. Скорректированы примеры запросов в методах «Старт верификации в ЕБС», «Согласование метода сбора БО и Liveness», «Приём БО на верификацию».
1.8	21/06/2018	Курочкин В.С.	Уточнена диаграмма состояний API биометрической верификации с использованием в качестве ДКО WEB-приложения.
1.7	19/06/2018	Курочкин В.С.	Скорректированы разделы: – 4.1.1 Технические рекомендации к оборудованию для получение биометрических образцов в офисе кредитной организации; – 4.1.4 Требования к предоставляемым биометрическим образцам. Уточнена диаграмма состояний API биометрической верификации с использованием в качестве ДКО WEB-приложения.
1.6	15/06/2018	Курочкин В.С.	1. Скорректированы схемы и описания бизнес-процессов с использованием в качестве ДКО web или мобильного приложения; 2. Скорректирована общая схема и описание взаимодействия при удаленной идентификации; 3. Добавлены требования к мобильному приложению КО; 4. Скорректировано описание API биометрической верификации; 5. Скорректировано Приложение Б. 6. Скорректировано Приложение В.
1.5	20/04/2018	Шульженко С.Н.	1. Удалено Приложение «Руководство пользователя по работе с библиотеками контроля качества»;

			2. Изменены сценарии и схемы API верификации; 3. В Приложение Б добавлены методы «Получение конфигурации API ЕБС» и «Получение результата верификации»; 4. Добавлено Приложение В. Описание установки и настройки МП ЕБС.
1.4	14/03/2018	Шульженко С.Н.	Раздел 4.2.1 внесено название scope «bio»
1.3	26/02/2018	Ваничков В.Н.	Обновлено описание Вида сведений «Прием заявлений на биометрическую регистрацию» к версии 1.2.0. Изменен пункт 4.1.4.2.1 в части заполнения метаданных.
1.2	29/01/2018	Шульженко С.Н.	1. Добавлен раздел 4.1.4.2.1 Рекомендации к произносимым последовательностям. 2. Добавлен раздел 4.1.2 Рекомендации по организации процесса сбора биометрических данных
1.1	10/01/2018	Шульженко С.Н.	Изменена структура документа. Добавлена диаграмма процесса удалённой идентификации с использованием биометрической верификации. Изменена схема ВС. Руководство пользователя по работе с БКК и API биометрической верификации вынесены в отдельные приложения. Рекомендации к выбору оборудования перенесены в основной текст документа.
1.0	25/09/2017	Долгиев А.А.	Создание документа

Содержание

Список сокращений

Термин	Определение
Адаптация биометрического контрольного шаблона	Обновление биометрического контрольного шаблона
Аутентификация	Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе
Бимодальный режим	Режим работы биометрической системы, при котором процесс биометрического распознавания происходит одновременно по каким-либо двум биометрическим характеристикам
Биометрическая верификация	Процесс подтверждения биометрического заявления при сравнении
Биометрическая проба	Биометрический образец или набор биометрических признаков, введённый в алгоритм для использования в качестве объекта сравнения с биометрическим контрольным шаблоном (биометрическими контрольными шаблонами)
Биометрическая регистрация	Действия по созданию и сохранению записи данных биометрической регистрации в соответствии с правилами биометрической регистрации
Биометрическая система	Система, предназначенная для биометрического распознавания людей, основанного на их поведенческих и биологических характеристиках
Биометрическая характеристика	Биологические и поведенческие характеристики человека, которые могут быть зарегистрированы и использованы в качестве отличительных, повторяющихся биометрических признаков для распознавания людей.

Термин	Определение
Биометрические данные	Биометрический образец или совокупность биометрических образцов на любой стадии обработки, например, биометрический контрольный шаблон, биометрическая проба, биометрический признак или биометрическое свойство
Биометрический контрольный шаблон (БКШ)	Один или более хранимых биометрических шаблонов, относящихся к субъекту биометрических данных и используемых в качестве объекта сравнения
Биометрический образец (БО)	Аналоговое или цифровое представление биометрических характеристик, предшествующее извлечению биометрических признаков
Биометрический признак	Цифровое представление информации (числа или метки), извлечённое из биометрических образцов и используемое для сравнения
Биометрический шаблон	Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками биометрической пробы
Биометрическое заявление	Заявление, что субъект сбора биометрических данных является или не является собственно источником установленного или неустановленного биометрического контрольного шаблона
Биометрия (биометрическое распознавание)	Распознавание человека, основанное на его поведенческих и биологических характеристиках.
Биометрический процессор	Обработчик запросов на выполнение биометрических операций.
ВС, Вид сведений (СМЭВ)	Протокол передачи сведений определённого вида между информационной системой поставщика и информационной системой потребителя

Термин	Определение
Вендор	Участник биометрического взаимодействия (юридическое лицо), осуществляющее техническую реализацию биометрического распознавания
Вероятность ложного совпадения	Вероятность того, что шаблон, извлечённый из предоставленного образца, будет ошибочно признан совпадающим с соответствующим контрольным шаблоном
Дистанционная идентификация	Идентификация пользователей, в рамках требований Федерального закона от 07.08.2001 №115-ФЗ, осуществляемая по удалённым каналам связи, без визита пользователя в офис кредитной организации
Запись данных биометрической регистрации	Запись данных, связанная с субъектом биометрических данных, содержащая не биометрические данные, и связанная с идентификатором (идентификаторами) биометрического контрольного шаблона
Идентификатор биометрического контрольного шаблона	Указатель на запись данных биометрического контрольного шаблона в базе данных биометрических контрольных шаблонов
Инфраструктура электронного правительства (ИЭП, e-Government)	Совокупность аппаратного и программного обеспечения для предоставления информации и оказания государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано и максимально возможно используются информационные технологии.

Термин	Определение
ИС Поставщика БДн	Информационная система организации, зарегистрированная в ЕБС, и имеющая возможность осуществлять сбор и предоставление БДн для биометрической регистрации
ИС Потребителя БДн	Информационная система организации, зарегистрированная в ЕБС, и имеющая возможность осуществлять сбор и предоставление БДн для биометрической верификации
Конечный пользователь, Пользователь ЕБС	Человек, взаимодействующий с биометрической системой с целью регистрации или идентификации его личности
Живучесть (Лайвнесс) / Liveness	Качество или признаки жизни субъекта, выявленные анатомическими характеристиками, непроизвольными реакциями, физиологическими функциями, добровольными реакциями, или поведением субъекта
Обнаружение живучести / Liveness detection	Измерение и анализ анатомических характеристик, непроизвольных или добровольных реакций субъекта для определения, собран ли биометрический образец с живого субъекта, присутствующего в точке захвата биометрического образца
Мульти модальная биометрическая система	Биометрическая система, работающая как минимум с двумя различными биометрическими характеристиками
Минкомсвязь России	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации — федеральный орган исполнительной власти в ведении Правительства Российской Федерации.
Национальная биометрическая платформа (ЕБС)	Система, обеспечивающая сбор, хранение, обработку и передачу биометрических данных человека

Термин	Определение
Оператор биометрической регистрации	Сотрудник Поставщика БДн, уполномоченный осуществлять процедуру биометрической регистрации
Поставщик БДн (ЕБС)	Участник биометрического взаимодействия, имеющий право и осуществляющий регистрацию Пользователей в ЕБС.
Потребитель БДн (ЕБС)	Участник биометрического взаимодействия, имеющий право и осуществляющий удаленную идентификацию Пользователей с использованием верификации биометрических данных в ЕБС.
Провайдер идентификации / Identity Provider (IdP)	Информационная система, отвечающая за взаимодействие системы управления учётными записями пользователей
Сбор биометрических данных	Получение и запись в воспроизводимой форме сигнала биометрической характеристики (биометрических характеристик) непосредственно от человека, или от представления биометрической характеристики (биометрических характеристик)
Сравнение	Оценка, вычисление или измерение степени схожести и различия между биометрическим образцом и биометрическим контрольным шаблоном
Степень схожести	Количественный показатель, характеризующий схожесть извлеченных из биометрического образца признаков с биометрическим контрольным шаблоном.
Транзакция биометрической верификации	Одна или более попыток биометрической верификации, результатом которых является заключение о биометрическом заявлении

Термин	Определение
Транзакция сбора биометрических данных	Одна или более попыток сбора биометрических данных с целью получения всех биометрических данных от субъекта биометрических данных, необходимых для создания биометрического контрольного шаблона или биометрической пробы
Унимодальный режим	Режим работы биометрической системы, при котором процесс биометрического распознавания происходит по какой-либо одной биометрической характеристике (например, по записи голоса)
Участник БВ	Участник биометрического взаимодействия имеющий право осуществлять регистрацию и/или верификацию биометрических данных в соответствии с ФЗ-115. А также поставщики биометрических процессоров (вендоры)
ID	Уникальный идентификатор учётной записи в ИС
HSM	Аппаратное устройство с предустановленным микроядром ОС и ПО, осуществляющее криптографические операции и процедуры
Web (Веб) приложение	Клиент-серверное приложение, в котором клиентом выступает интернет браузер, а сервером — интернет-сервер
XML	Расширяемый язык разметки текстовых документов
БД	База данных
БДн	Биометрические данные
БКК	Библиотека контроля качества
БКШ	Биометрический контрольный шаблон
БО	Биометрические образцы
ВС	Вид сведений СМЭВ
ДКО	Дистанционные каналы обслуживания (WEB и мобильные приложения)
ИС	Информационная система
ИЭП	Инфраструктура электронного правительства

Термин	Определение
КВ2	Уровень защиты информации в соответствии с Приказ ФСБ России от 10.07.2014 N 378
КО	Кредитные организации
КЭП	Квалифицированная электронная подпись
КЭП ЭП-ОВ	Квалифицированная электронная подпись органа власти (ЭП-ОВ). Необходима для подписания запросов ИС Поставщика БДн через СМЭВ
ЕБС, Система	Национальная биометрическая платформа
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПОД/ФТ	Противодействие легализации (Отмыванию) Доходов, полученных преступным путём, и Финансированию Терроризма
РФ	Российская Федерация
СПО	Системное программное обеспечение - комплекс программ, которые обеспечивают управление компонентами компьютерной системы, выступая как «межслойный интерфейс», с одной стороны которого аппаратура, а с другой — приложения пользователя.
СМЭВ 3.х	Система межведомственного электронного взаимодействия, функционирующего по методическим рекомендациям версии 3.х
УЗ	Учётная запись

Термин	Определение
ФГИС ЕСИА, ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ФГИС СМЭВ, СМЭВ	Федеральная государственная информационная Система Межведомственного Электронного Взаимодействия

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:

- Подключение к ЕБС Участников биометрического взаимодействия;
- Рекомендации по реализации интеграции Участника биометрического взаимодействия (ИС Поставщика и Потребителя БДн) с ЕБС;
- Процесс регистрации биометрических данных;
- Процесс верификации биометрических данных;
- Рекомендации к выбору оборудования;
- Требования к ИС Поставщика и Потребителя БДн.

Описываемые в документе правила являются обязательными к применению участниками биометрического взаимодействия ЕБС с использованием системы межведомственного электронного взаимодействия (СМЭВ 3.xx) и единой системы идентификации и аутентификации (ЕСИА).

Для описания требований к участникам взаимодействия используются следующие соглашения, выделенные жирным шрифтом:

- **может** – разрешено, но необязательно;
- **не может** – запрещено;
- **должен** – обязательно.

1.2 Нормативные ссылки

Данный документ разработан в целях реализации и во исполнение:

- Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» (в редакции Федерального закона РФ от 31.12.2017 №482-ФЗ);
- Федерального закона от 07.07.2003 № 126-ФЗ «О связи».

2 ОБЩЕЕ ОПИСАНИЕ СИСТЕМЫ

Целью создания Системы является обеспечение возможности проведения удалённой биометрической верификации пользователей по биометрическим характеристикам для исполнения требований, установленных федеральными законами от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ) и от 07.07.2003 № 126-ФЗ «О связи» (далее – Федеральный закон № 126-ФЗ).

Система обеспечивает уровень надёжности, необходимый для удалённой идентификацию физических лиц кредитными организациями (КО) – потребителями БДн, с дальнейшим оказанием им банковских услуг.

Система обеспечивает возможность решения следующих задач:

1. Сбор биометрических данных как в офисах КО – поставщиков БДн, так и удалённо;
2. Передачу биометрических образцов от КО - поставщиков БДн в ЕБС;
3. Хранение в Системе биометрических образцов;
4. Формирование из биометрических образцов биометрических шаблонов с приданием им статуса биометрических контрольных шаблонов;
5. Хранение в Системе биометрических контрольных шаблонов;
6. Получение биометрических образцов от пользователей через ДКО КО - потребителей БДн;
7. Проверку полученных биометрических образцов на соответствие качеству и защиты от попыток фальсификации;
8. Сравнение биометрических образцов с биометрическими контрольными шаблонами для проведения процедуры биометрической верификации в ЕБС;
9. Взаимодействие ЕБС с ДКО КО - потребителей БДн;
10. Взаимодействие ЕБС с ЕСИА и СМЭВ.

Разработанная Система обеспечивает мульти модальный режим работы. Список биометрических характеристик (модальностей), используемых для осуществления процесса верификации состоит из следующих модальностей:

- модальность 1: аудиозапись голоса;
- модальность 2: фотоизображение лица.

3 ОСНОВЫ ВЗАИМОДЕЙСТВИЯ

3.1 Описание процесса «Регистрация биометрических данных в ЕБС»

Для получения возможности прохождения удалённой идентификации через ДКО КО - Потребителей БДн, пользователь, должен лично обратиться в КО – Поставщика БДн, имеющей право проводить биометрическую регистрацию, с целью прохождения процедуры биометрической регистрации. Список Участников БВ, имеющих право проводить полную биометрическую регистрацию устанавливается нормативными документами.

В соответствии с требованиями пункта 25 Приказа Минкомсвязи России «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации», процесс биометрической регистрации физического лица в ЕБС должен сопровождаться идентификацией физического лица в ЕСИА, и не может быть осуществлён частично. Диаграмма процесса биометрической регистрации с использованием СМЭВ 3.xx представлена на рисунке ниже (см. Рисунок 1).

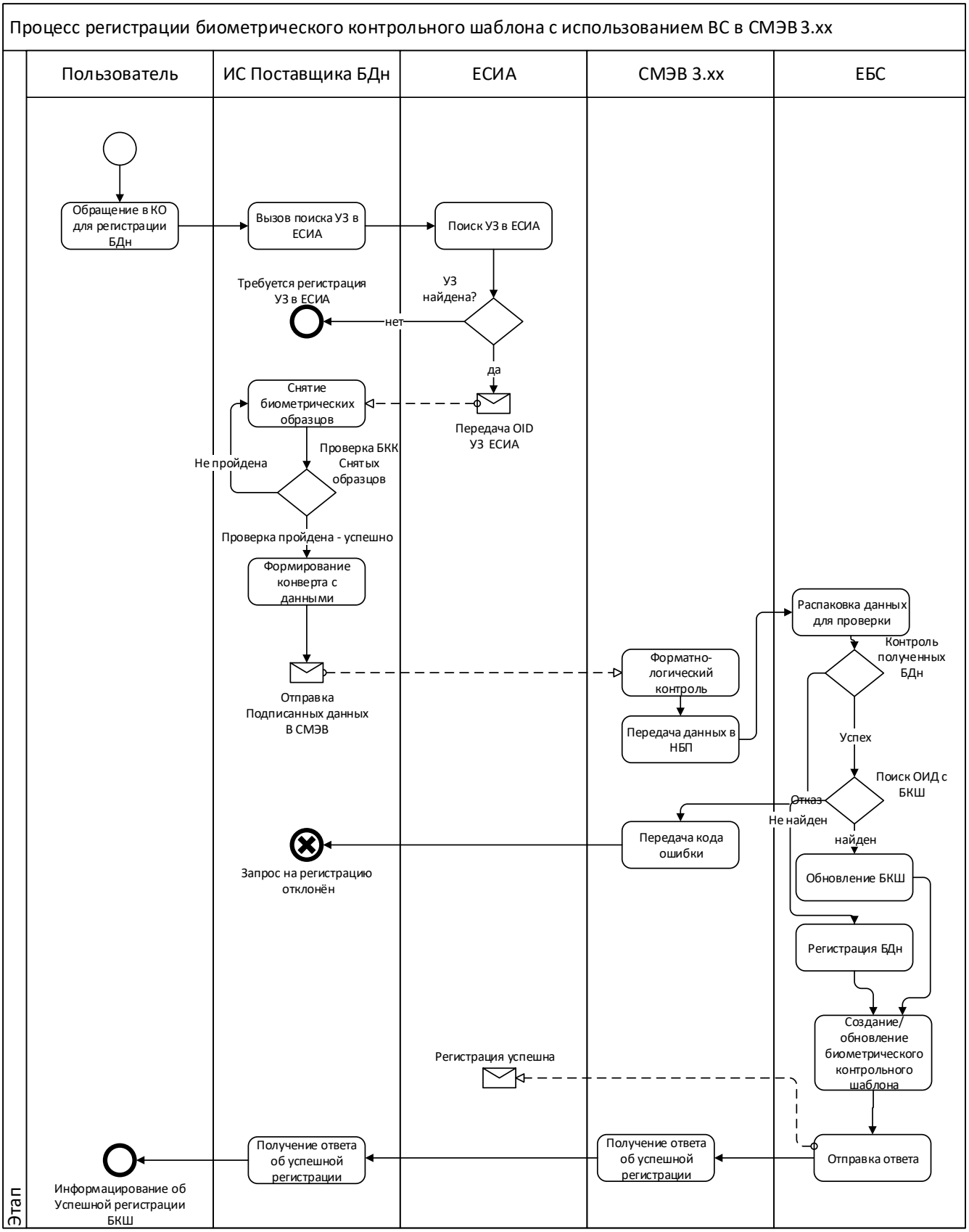

Рисунок 1 – Процесс биометрической регистрации с использованием СМЭВ 3.xx

Пользователь обращается в офис КО - Поставщика БДн для регистрации БДн. Оператор биометрической регистрации, на основании паспортных данных клиента, с использованием механизмов создания/проверки учетной записи ЕСИА, проверяет статус учетной записи (УЗ) клиента в ЕСИА.

В случае, если учетная запись физического лица не является подтвержденной, Поставщик БДн передает в ЕСИА недостающие персональные данные и производит процедуру регистрации подтвержденной учетной записи пользователя на базе существующей упрощенной или стандартной учетной записи ЕСИА, согласно разделу 3.6 «Руководства оператора центра обслуживания ЕСИА[1]»

Если ЕСИА подтверждает отсутствие учетной записи физического лица, то Поставщик БДн производит процедуру регистрации подтвержденной учетной записи пользователя с созданием новой учетной записи ЕСИА, согласно разделу 3.5 «Руководства оператора центра обслуживания ЕСИА»

После того, как Оператор биометрической регистрации завершил процедуру создания или подтверждения УЗ, не дожидаясь ответа от ЕСИА, можно приступить к сбору биометрических данных. Для этого Оператор биометрической регистрации, используя интерфейс ИС Поставщика БДн для сбора биометрических данных, разработанной Поставщиком БДн самостоятельно, делает аудиозапись голоса клиента и фотографию его лица. Полученные биометрические образцы должны проверяться на соответствие требованиям качества с помощью библиотеки контроля качества, поставляемой ЕБС.

После того, как Оператор биометрической регистрации удостоверится в том, что качество полученных биометрических образцов соответствует требованиям ЕБС, данные биометрические образцы и идентификатор УЗ ЕСИА передаются в ЕБС.

Для Поставщика БДн процесс взаимодействия с пользователем с целью Адаптации БКШ, полностью идентичен процессу взаимодействия с пользователем при биометрической регистрации. В ЕБС сохранится признак, что была произведена Адаптация БКШ, если БДн пользователя ранее регистрировались.

[1] http://minsvyaz.ru/ru/documents/4247/

Передача биометрических образцов из ИС Поставщика БДн в ЕБС должна осуществляться с использованием Единой системы межведомственного электронного взаимодействия (СМЭВ 3.xx) в соответствии с действующими Методическими рекомендациями по работе с Единой системой межведомственного электронного взаимодействия (СМЭВ 3.xx) и документом «Универсальный ВС для приема заявлений на биометрическую регистрацию».

В ЕБС на основании предоставленных Поставщиком БДн биометрических образцов создается биометрический контрольный шаблон, который привязывается к идентификатору УЗ ЕСИА. У созданной/обновленной учетной записи ЕСИА устанавливается дополнительный признак наличия биометрических данных.

Возможно проведение биометрической регистрации вне офиса Поставщика БДн силами Оператора биометрической регистрации, выезжающего на встречу с клиентом. Процедура аналогична Процедуре биометрической регистрации в офисе Поставщика БДн. При этом часть функций, связанных со сбором биометрических данных, выполняется программным обеспечением, развёрнутым на мобильных устройствах оператора биометрической регистрации и использующимся для регистрации заявок на получение услуг Поставщика БДн. Проверка паспортных данных производится Оператором биометрической регистрации.

ВНИМАНИЕ! Обязательным условием возможности прохождения удаленной идентификации Пользователя с использованием биометрических данных является наличие УЗ Пользователя ЕСИА со статусом «Подтвержденная».

По окончанию создания БКШ в ЕБС и соответствию статуса УЗ ЕСИА «Подтверждённая», ЕСИА информирует пользователя путем отображения соответствующего статуса в личном кабинете пользователя ЕСИА об изменении статуса его УЗ ЕСИА.

Бизнес сценарий биометрической регистрации приведён в таблице ниже (см. Таблица 1).

Таблица 1 Бизнес сценарий биометрической регистрации

Система: ЕБС

Роли:

- Оператор биометрической регистрации – основное действующее лицо;
- Пользователь сервиса - дополнительное действующее лицо;
- Участник биометрического взаимодействия, являющийся Поставщиком БДн - дополнительное действующее лицо.

Предварительные условия:

- Личное присутствие гражданина РФ (Пользователь сервиса);
- Согласие гражданина (Пользователь сервиса) на биометрическую регистрацию;
- Участник биометрического взаимодействия зарегистрирован в ЕБС в роли Поставщика БДн;
- Участник биометрического взаимодействия зарегистрирован в СМЭВ 3.xx;
- Участник биометрического взаимодействия зарегистрирован у Провайдера идентификации (ЕСИА).

Выходные условия:

- Выполнена биометрическая регистрация / адаптация БКШ гражданина РФ (Пользователь сервиса);

Заинтересованные лица:

Оператор журналирования и аудита:

- наличие записей в журнале о попытках регистрации и их статусах выполнения.
- наличие записей в журнале о попытках перерегистрации БКШ и их статусах выполнения.

Инициирующее событие:

- Обращение гражданина РФ (Пользователь сервиса) за услугой к Поставщику БДн.

Основной сценарий

Шаг 1. Оператор ИС организации - поставщика БДн осуществляет поиск учетной записи у провайдера идентификации(ЕСИА). УЗ найдена, получен OID УЗ ЕСИА.

Шаг 2. Оператор ИС Поставщика БДн фотографирует Пользователя сервиса и осуществляет аудиозапись его голоса.

Шаг 3. ИС Поставщика БДн с использованием предоставляемой БКК проверяет качество фото и аудиозаписи (биометрических образцов далее БО).

Шаг 4. ИС Поставщика БДн формирует запрос на регистрацию БДн, подписывает его КЭП ЭП-ОВ и отправляет в СМЭВ 3.х.

Шаг 5. СМЭВ 3.х проводит форматно-логический контроль входящего запроса на регистрацию БКШ;

Шаг 6. ЕБС получает запрос из СМЭВ, авторизует ИС организации - Поставщика БДн по КЭП.

Шаг 7. ЕБС проводит регистрацию/адаптацию БКШ.

Шаг 8. ЕБС уведомляет Провайдера идентификации (ЕСИА) об успешной регистрации Пользователя сервиса.

Шаг 9. ЕБС отправляет в СМЭВ сообщение о результатах регистрации БДн для ИС поставщика БДн.

Шаг 10. СМЭВ отправляет в очередь сообщений для ИС Поставщика БДн сообщение об успешной регистрации БДн в ЕБС.

Альтернативные сценарии

Шаг 1а. Учетная запись не найдена.

Шаг 1а1. Оператор ИС поставщика БДн производит регистрацию подтвержденной УЗ пользователя с созданием новой УЗ в соответствии с действующей версией Руководства оператора ЦО.
Шаг 1а2. Переход к шагу 2.

Шаг 1б. Учетная запись не является «Подтвержденной».

Шаг 1б1. Оператор ИС поставщика БДн производит подтверждение УЗ или регистрацию подтвержденной УЗ пользователя на базе существующей упрощенной УЗ пользователя в соответствии с действующей версией Руководства оператора ЦО.

Шаг 1б2. Переход к шагу 2.

Шаг 3а. Проверка качества БО не пройдена

Шаг 3а1. Оператор ИС поставщика БДн проводит повторную операцию сбора биометрических образцов.
Шаг 3а2. Возврат на шаг 3.

Исключительные сценарии

Шаг 5а. Форматно-логический контроль не пройден

Шаг 5а1. ФЛК в СМЭВ не пройден.

Шаг 5а2. Прекращение сценария.

Шаг 6а. Авторизация ИС поставщика БДн не пройдена

Шаг 6а1. ЕБС отправляет в СМЭВ сообщение для ИС поставщика
Шаг 6а2. Прекращение сценария.

Список технологий и типов данных:

Для снятия БДн используются веб-камера и микрофон.

- Две модальности: фото и аудиозапись голоса

3.2 Описание процесса «Удаленная идентификация с использованием биометрической верификации ЕБС»

Процедура удалённой идентификации включает последовательное прохождение аутентификации в ЕСИА по логину/паролю и верификации в ЕБС по степени схожести биометрического образца.

Для обеспечения процедуры удалённой идентификации используются:

- механизм аутентификации пользователей ЕСИА, для обеспечения возможности запросить усиленную аутентификацию с помощью биометрической верификации, обеспечиваемую ЕБС;
- компонент ЕБС для сбора БО:
    - в случае использования WEB-приложения Потребителя БДн, снятие БО производит WEB-форма ЕБС;
    - в случае использования мобильного приложения Потребителя БДн, снятие БО производит МП ЕБС;
- SDK ЕБС (далее SDK) используется для встраивания в стороннее мобильное приложение Потребителя БДн, и обеспечивает:
    - проверку наличия мобильного приложения для удалённой идентификации (МП ЕБС);
    - взаимодействие МП Потребителя БДн и МП ЕБС для биометрической верификации
- универсальный механизм (API-биометрической верификации) ЕБС, для обеспечения возможности подключения внешних систем к ЕБС.

После успешного прохождения процедуры аутентификации в ЕСИА, собранные биометрические образцы передаются в API-биометрической верификации ЕБС.

На этапе биометрической верификации в ЕБС, в активированных биометрических процессорах соответствующей модальности, создаётся биометрическая проба, состоящая из предоставленных биометрических образцов и созданных, из биометрических образцов, моделей – биометрических признаков. Биометрическая проба сравнивается с биометрическими шаблонами соответствующих биометрических процессоров, биометрического контрольного шаблона, находящимся в хранилище биометрических данных пользователей. Результатом верификации является:

- расчёт значения степени схожести биометрической пробы и соответствующего биометрического шаблона в составе:

- результат вычитания из единицы вероятности ложного совпадения по каждой биометрической модальности;
- результат вычитания из единицы суммарной вероятности ложного совпадения;

- передача результатов сравнения во внешнюю систему.

ЕБС возвращает положительный расширенный результат в ИС-Потребителя БДн, если вероятность ложного совпадения не превышает установленный Правительством РФ по согласованию с ЦБ минимальный порог. В ином случае возвращается отказ. Диаграмма процесса удаленной регистрации с использованием биометрической верификации ЕБС представлена на рисунках ниже (см. Рисунок 2 и Рисунок 3).

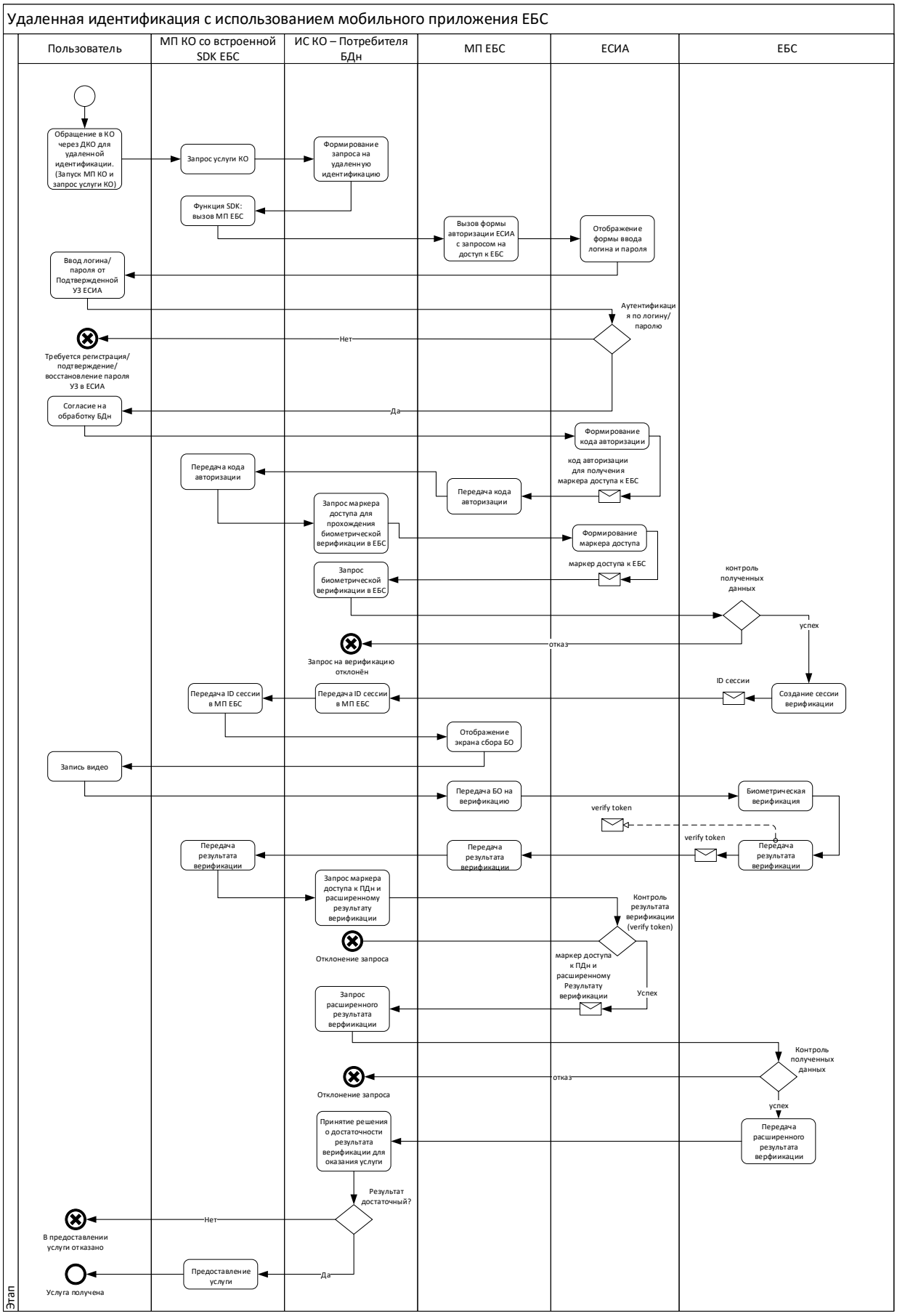

Рисунок 2 – Процесс удаленной идентификации с использованием МП ЕБС

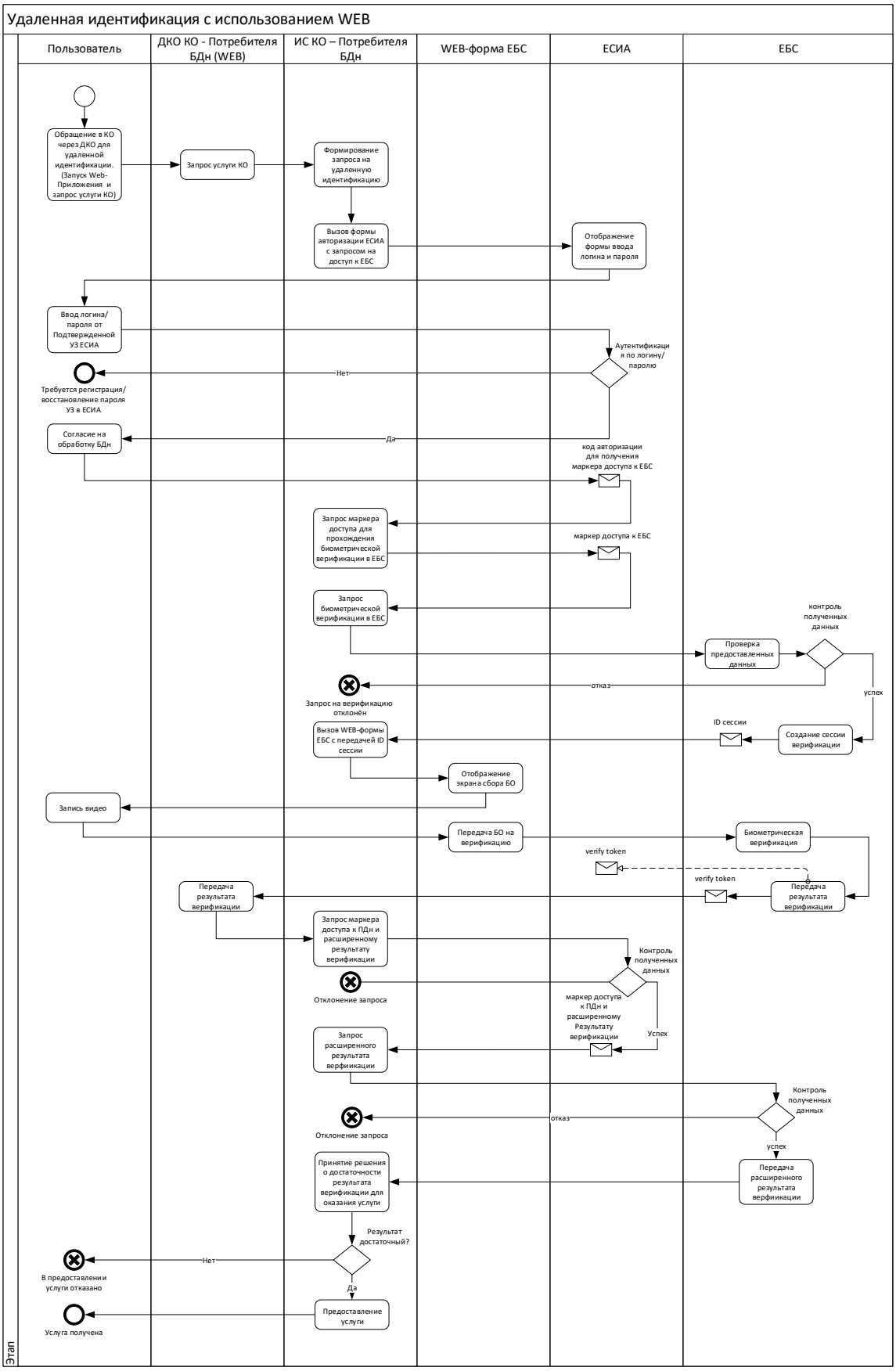

Рисунок 3 – Процесс удаленной идентификации с использованием Web

Бизнес сценарий биометрической верификации приведён в таблицах ниже (см. Таблица 2, Таблица 3).

Таблица 2 Бизнес сценарий биометрической верификации (запрос с мобильного приложения)

Система: ЕБС

Роли:

- Пользователь сервиса - основное действующее лицо;
- ИС организаций - потребителя БДн - дополнительное действующее лицо (далее "ИС Потребителя БДн");
- ЕСИА;
- ЕБС.

Предварительные условия:

- Использование гражданином РФ (Пользователь сервиса) мобильного приложения ИС Потребителя БДн (далее "МП ИС Потребителя БДн") со встроенной SDK ЕБС;
- Использование гражданином РФ (Пользователь сервиса) мобильного приложения ЕБС (далее "МП ЕБС");
- Согласие гражданина РФ (Пользователь сервиса) на предоставление биометрических данных;
- Пользователь сервиса имеет подтвержденную УЗ ЕСИА;
- Участник биометрического взаимодействия зарегистрирован в ЕБС в роли Потребителя БДн;
- Участник биометрического взаимодействия зарегистрирован в ЕСИА;
- Наличие камеры и микрофона на устройстве пользователя.

Выходные условия:

Выполнена биометрическая верификация гражданина РФ (Пользователь сервиса);

Заинтересованные лица:

ИС-Потребителя БДн:

- Пользователь сервиса идентифицирован в ЕСИА и прошел биометрическую верификацию в ЕБС;
- Получен доступ к ПДн Пользователя сервиса в ЕСИА.

Пользователь сервиса:

– получение запрашиваемой услуги

Инициирующее событие:

Обращение гражданина РФ (Пользователь сервиса) за услугой к Участнику биометрического взаимодействия, который является зарегистрированным Потребителем БДн в ЕБС, через МП ИС Потребителя БДн

Основной сценарий:

Шаг 1. Пользователь сервиса в МП ИС Потребителя БДн выбирает получение услуги, требующей усиленной аутентификации, и инициирует идентификацию с биометрической верификацией.

Шаг 2. МП ИС Потребителя БДн формирует и подписывает в Backend Потребителя БДн запрос и обращается к SDK ЕБС.

Шаг 3. SDK ЕБС вызывает МП ЕБС, передав подписанный запрос

Шаг 4. МП ЕБС перенаправляет Пользователя на страницу аутентификации ЕСИА (webview).

Шаг 5. Пользователь сервиса проходит аутентификацию в ЕСИА.

Шаг 6. ЕСИА проверяет статус УЗ пользователя (для осуществления биометрической аутентификации УЗ должна иметь статус «Подтвержденная»).

Шаг 7. Пользователь дает согласие на проведение усиленной аутентификации с использованием его биометрических данных.

Шаг 8. После успешной аутентификации Пользователя, ЕСИА возвращает в МП ЕБС код авторизации для получения маркера доступа для прохождения биометрической верификации в ЕБС.

Шаг 9: МП ЕБС возвращает код авторизации в МП ИС Потребителя БДн.

Шаг 10: МП ИС Потребителя передает код авторизации в Backend ИС Потребителя БДн. Backend ИС Потребителя БДн обращается в ЕСИА за маркером доступа для прохождения биометрической верификации в ЕБС, предъявив полученный код авторизации.

Шаг 11: Backend ИС Потребителя БДн передает запрос на старт биометрической верификации в ЕБС, предъявляя полученный маркер доступа.

Шаг 12. ЕБС производит проверку из полученного маркера доступа:

– подписи ЕСИА на полученном маркере доступа;

– статуса ИС Потребителя БДн по предоставленной мнемонике;

– статуса биометрических данных Пользователя по предоставленному OID.

Шаг 13. ЕБС создает сессию верификации и возвращает в backend ИС Потребителя БДн сообщение по протоколу HTTP содержащее: код состояния 302(для API версии v1) или 200 (для API версии v2), идентификатор сессии, заданное значение времени жизни сессии, URL WEB-формы получения БО.

Шаг 14: Backend ИС Потребителя БДн через МП ИС Потребителя БДн передает ID сессии в МП ЕБС.

Шаг 15. МП ЕБС отображает Пользователю страницу съема биометрии, содержащую полученную из ЕБС действие liveness и инструкцию по формированию биометрических образцов.

Шаг 16. Пользователь сервиса на странице съема биометрии формирует биометрические образцы: производит запись видео, выполнив действия, согласно отображенной инструкции.

Шаг 17. МП ЕБС передаёт полученные биометрические образцы (видеоролик) в ЕБС.

Шаг 18. ЕБС сохраняет полученные биометрические образцы.

Шаг 19. ЕБС осуществляет проверку liveness и верифицирует Пользователя.

Шаг 20. ЕБС передает результат биометрической верификации в ЕСИА (по ссылке, указанной в маркере доступа) и уникальный идентификатор (verifyToken).

Шаг 21. ЕБС возвращает обобщенный результат прохождения биометрической верификации Пользователя (успешно или неуспешно) и уникальный идентификатор (verifyToken), аналогичный переданному в ЕСИА, в МП ЕБС. МП ЕБС возвращает в МП ИС Потребителя БДн через SDK ЕБС полученный результат верификации и параметры verifyToken.

Шаг 22. МП Потребителя БДн передает полученный результат в backend ИС Потребителя БДн.

Шаг 23. Backend ИС Потребителя БДн обращается к ЕСИА с запросом, содержащим в том числе полученный от ЕБС уникальный идентификатор (verifyToken), на доступ к персональным данным.

Шаг 24. ЕСИА проверяет возможность предоставления ИС Потребителя БДн доступа к персональным данным сравнивая полученные verifyToken от ЕБС и ИС-Потребителя БДн.

Шаг 25. ЕСИА запрашивает у Пользователя сервиса разрешение на предоставление ИС-Потребителю БДн доступа к персональным данным пользователя.

Шаг 26. Пользователь сервиса подтверждает согласие на передачу персональных данных.

Шаг 27. ЕСИА предоставляет в backend ИС Потребителя БДн специальный маркер доступа для получения персональных данных Пользователя.

Шаг 28. ИС Потребителя БДн обращается к ЕБС с запросом, содержащим в том числе полученный от содержащим в том числе полученный от ЕСИА, на Шаге 27 основного сценария, специальный маркер доступа, на получение расширенного результата верификации.

Шаг 29. ЕБС проверяет возможность предоставления ИС Потребителя БДн расширенного результата верификации.

Шаг 30. ЕБС передает в backend ИС Потребителя БДн расширенный результат биометрической верификации Пользователя.

Шаг 31. Backend ИС Потребителя БДн принимает положительное решение о результате усиленной аутентификации с биометрической верификацией и оказывает услугу Пользователю сервиса.

Альтернативные сценарии:

Отсутствуют

Исключительные сценарии:

Исключительный сценарий 1 - МП ЕБС не установлено на устройстве Пользователя:

Шаг 3а. Проверка не выявила наличия установленного на устройстве Пользователя МП ЕБС.

Шаг 3а.1. Пользователю выдается предложение установить МП ЕБС с ссылкой на точку распространения программного обеспечения для мобильных устройств.

Завершение сценария

Исключительный сценарий 2 – Пользователь не прошел аутентификацию в ЕСИА:

Шаг 5а. Пользователь не прошел аутентификацию в ЕСИА.

Завершение сценария

Исключительный сценарий 3 – УЗ пользователя не является подтвержденной:

Шаг 6а.1 ЕСИА проверяет статус УЗ пользователя и выявляет, что УЗ пользователя не является подтвержденной УЗ.

Шаг 6а.2 Пользователю выдается ошибка о невозможности аутентификации из-за недостаточного уровня УЗ.

Завершение сценария

Исключительный сценарий 4 – Пользователь не предоставил разрешение на усиленную аутентификацию с использованием биометрии:

Шаг 7а.1 ЕСИА не получает согласия Пользователя биометрическую верификацию.

Завершение сценария

Исключительный сценарий 5 – ИС Потребителя БДн не зарегистрирована в ЕБС:

Шаг 12а.1 ЕБС проверяет регистрацию и статус ИС Потребителя БДн по предоставленной мнемонике.

Шаг 12а.2 ЕБС возвращает ответ, о том, что ИС не зарегистрирована в качестве Потребителя БДн

Шаг 12а.3 Пользователю выдается ошибка о невозможности усиленной аутентификации.

Завершение сценария

Исключительный сценарий 6 – Биометрические данные по предоставленному OID отсутствуют:

Шаг 12б.1 ЕБС проверяет статус биометрических данных Пользователя по предоставленному OID.

Шаг 12б.2 ЕБС возвращает ответ, о том, что по данному OID нет активных биометрических данных.

Шаг 12б.3 Пользователю выдается ошибка о невозможности усиленной аутентификации из-за блокировки биометрических данных.

Завершение сценария

Исключительный сценарий 7 – Биометрические образцы не прошли верификацию:

Шаг 19а.1 ЕБС осуществляет проверку liveness и верифицирует полученные биометрические образцы.

Шаг 19а.2 ЕБС возвращает отрицательный результат биометрической верификации в ЕСИА и в МП ИС Потребителя БДн. Ответ с отрицательным результатом не содержит verifyToken.

Шаг 19а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Исключительный сценарий 8 – При обращении в ЕСИА ИС Потребителя БДн не передал значение verifyToken:

Шаг 23а.1 При обращении в ЕСИА ИС Потребителя БДн не передал значение verifyToken.

Шаг 23а.2 ЕСИА возвращает ответ с сообщением об ошибке проведения усиленной аутентификации.

Шаг 23а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Исключительный сценарий 9 – Значение verifyToken при обращении ИС-Потребителя БДн в ЕСИА не совпало с указанным ЕБС в полученном результате верификации:

Шаг 24а.1 При проверке ЕСИА возможности предоставления ИС Потребителя БДн доступа к персональным данным, значение verifyToken, при обращении ИС Потребителя БДн, не совпало с указанным ЕБС в полученном результате верификации.

Шаг 24а.2 ЕСИА возвращает ответ с сообщением об ошибке проведения усиленной аутентификации.

Шаг 24а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Исключительный сценарий 9 – Пользователь не подтвердил свое согласие на передачу персональных данных:

Шаг 26а.1 При запросе подтверждения Пользователем сервиса передачи персональных данных, ЕСИА получен отрицательный ответ.

Шаг 26а.2 ЕСИА возвращает ответ с сообщением об ошибке проведения усиленной аутентификации.

Шаг 26а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Список технологий и типов данных:

Приложение ДКО: мобильное приложение iOS (не ниже 10 версии) или мобильное приложение Android (не ниже версии 5).

Таблица 3 Бизнес сценарий биометрической верификации (запрос с WEB-приложения)

Система: ЕБС

Роли:

- Пользователь сервиса - основное действующее лицо;
- ИС организаций - потребителя БДн - дополнительное действующее лицо (далее "ИС Потребителя БДн");
- ЕСИА;
- ЕБС.

Предварительные условия:

- Использование гражданином РФ (Пользователь сервиса) web-приложения ИС Потребителя БДн;
- Согласие гражданина РФ (Пользователь сервиса) на предоставление биометрических данных;
- Пользователь сервиса имеет подтвержденную УЗ ЕСИА;
- Участник биометрического взаимодействия зарегистрирован в ЕБС в роли Потребителя БДн;
- Участник биометрического взаимодействия зарегистрирован в ЕСИА;
- Наличие камеры и микрофона на устройстве пользователя[2].

Выходные условия:

Выполнена биометрическая верификация гражданина РФ (Пользователь сервиса);

Заинтересованные лица:

ИС Потребителя БДн:

[2] Проверку данного условия осуществляет WEB-форма ЕБС по съему БО

- Пользователь сервиса идентифицирован в ЕСИА и прошел биометрическую верификацию в ЕБС;
- Получен доступ к ПДн Пользователя сервиса в ЕСИА.

Пользователь сервиса:

- получение запрашиваемой услуги.

Инициирующее событие:

Обращение гражданина РФ (Пользователь сервиса) за услугой к Участнику биометрического взаимодействия, который является зарегистрированным Потребителем БДн в ЕБС, через web-приложение ИС Потребителя БДн

Основной сценарий:

Шаг 1. Пользователь сервиса в WEB-приложении ИС Потребителя БДн выбирает получение услуги, требующей усиленной аутентификации, и инициирует идентификацию с биометрической верификацией.

Шаг 2. Backend ИС Потребителя БДн формирует и подписывает запрос и перенаправляет Пользователя на страницу аутентификации ЕСИА.

Шаг 3. Пользователь сервиса проходит аутентификацию в ЕСИА.

Шаг 4. ЕСИА проверяет статус УЗ пользователя (для осуществления биометрической аутентификации УЗ должна иметь статус «Подтвержденная»).

Шаг 5. Пользователь дает согласие на проведение усиленной аутентификации с использованием его биометрических данных.

Шаг 6. После успешной аутентификации Пользователя в ЕСИА, ИС-Потребителя БДн получает от ЕСИА код авторизации для получения маркера доступа для прохождения биометрической верификации в ЕБС.

Шаг 7: ИС Потребителя БДн обращается в ЕСИА за маркером доступа для прохождения биометрической верификации в ЕБС, предъявив полученный код авторизации.

Шаг 8: ИС Потребителя БДн передает запрос на старт биометрической верификации в ЕБС, предъявляя полученный маркер доступа и URL ИС Потребителя БДн, на который ЕБС должна перенаправить Пользователя при положительном результате биометрической верификации.

Шаг 9. ЕБС производит проверку из полученного маркера доступа:

- подписи ЕСИА на полученном маркере доступа;
- статуса ИС-Потребителя БДн по предоставленной мнемонике;

– статуса биометрических данных Пользователя по предоставленному OID.

Шаг 10. ЕБС создает сессию верификации и возвращает в ИС Потребителя БДн сообщение по протоколу HTTP содержащее: код состояния 302 (для API версии v1) или 200 (для API версии v2), идентификатор сессии, заданное значение времени жизни сессии, URL WEB-формы получения БО.

Шаг 11. ИС Потребителя БДн отображает пользователю WEB-форму ЕБС съема биометрических данных (redirect) где Пользователь подтверждает свое согласие на биометрическую верификацию.

Шаг 12. WEB-форма съема биометрии отображает пользователю полученную из ЕБС действие liveness и инструкцию по формированию биометрических образцов.

Шаг 13. Пользователь сервиса на WEB-форме съема биометрии формирует биометрические образцы: производит запись видео, выполнив действия, согласно отображенной инструкции.

Шаг 14. ЕБС сохраняет полученные биометрические образцы.

Шаг 15. ЕБС осуществляет проверку liveness и верифицирует Пользователя.

Шаг 16. ЕБС передает результат биометрической верификации в ЕСИА (по ссылке, указанной в маркере доступа) и уникальный идентификатор (verifyToken).

Шаг 17. ЕБС перенаправляет Пользователя сервиса на URL, ранее указанный ИС Потребителя БДн в запросе (перенаправление содержит уникальный идентификатор (verifyToken), аналогичный переданному в ЕСИА).

Шаг 18. ИС Потребителя БДн обращается к ЕСИА с запросом, содержащим в том числе полученный от ЕБС уникальный идентификатор (verifyToken) на доступ к персональным данным.

Шаг 19. ЕСИА проверяет возможность предоставления ИС Потребителя БДн доступа к персональным данным сравнивая полученные verifyToken от ЕБС и ИС-Потребителя БДн.

Шаг 20. ЕСИА запрашивает у Пользователя сервиса разрешение на предоставление ИС-Потребителю БДн доступа к персональным данным пользователя.

Шаг 21. Пользователя сервиса подтверждает согласие на передачу персональных данных.

Шаг 22. ЕСИА предоставляет в Backend ИС-Потребителя БДн специальный маркер доступа для получения персональных данных Пользователя.

Шаг 23. ИС Потребителя БДн обращается к ЕБС с запросом, содержащим в том числе полученный от ЕСИА, на Шаге 22 основного сценария, специальный маркер доступа, на получение расширенного результата верификации.

Шаг 24. ЕБС проверяет возможность предоставления ИС Потребителя БДн расширенного результата верификации.

Шаг 25. ЕБС передает в Backend ИС Потребителя БДн расширенный результат биометрической верификации Пользователя.

Шаг 26. ИС-Потребителя БДн принимает положительное решение о результате усиленной аутентификации с биометрической верификацией и оказывает услугу Пользователю сервиса.

Альтернативные сценарии:

Отсутствуют

Исключительные сценарии:

Исключительный сценарий 1 – Пользователь не прошел аутентификацию в ЕСИА:

Шаг 3а. Пользователь не прошел аутентификацию в ЕСИА.

Завершение сценария

Исключительный сценарий 2 – УЗ пользователя не является подтвержденной:

Шаг 4а.1 ЕСИА проверяет статус УЗ пользователя и выявляет, что УЗ пользователя не является подтвержденной УЗ.

Шаг 4а.2 Пользователю выдается ошибка о невозможности аутентификации из-за недостаточного уровня УЗ.

Завершение сценария

Исключительный сценарий 3 – Пользователь не предоставил разрешение на усиленную аутентификацию с использованием биометрии:

Шаг 5а.1 ЕСИА не получает согласия Пользователя биометрическую верификацию.

Завершение сценария

Исключительный сценарий 4 – ИС Потребителя БДн не зарегистрирована в ЕБС:

Шаг 9а.1 ЕБС проверяет регистрацию и статус ИС-Потребителя БДн по предоставленной мнемонике.

Шаг 9а.2 ЕБС возвращает ответ, о том, что ИС не зарегистрирована в качестве Потребителя БДн

Шаг 9а.3 Пользователю выдается ошибка о невозможности усиленной аутентификации.

Завершение сценария

Исключительный сценарий 5 – Биометрические данные по предоставленному OID отсутствуют:

Шаг 9б.1 ЕБС проверяет статус биометрических данных Пользователя по предоставленному OID.

Шаг 9б.2 ЕБС возвращает ответ, о том, что по данному OID нет активных биометрических данных.

Шаг 9б.3 Пользователю выдается ошибка о невозможности усиленной аутентификации из-за блокировки биометрических данных.

Завершение сценария

Исключительный сценарий 6 – Биометрические образцы не прошли верификацию:

Шаг 15а.1 ЕБС осуществляет проверку liveness верифицирует полученные биометрические образцы.

Шаг 15а.2 ЕБС возвращает отрицательный результат биометрической верификации в ЕСИА и Web-приложение ИС Потребителя БДн. Ответ с отрицательным результатом не содержит verifyToken.

Шаг 15а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Исключительный сценарий 7 – При повторном обращении в ЕСИА ИС-Потребителя БДн не передал значение verifyToken:

Шаг 18а.1 При повторном обращении в ЕСИА ИС-Потребителя БДн не передал значение verifyToken.

Шаг 18а.2 ЕСИА возвращает ответ с сообщением об ошибке проведения усиленной аутентификации.

Шаг 18а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Исключительный сценарий 8 – Значение verifyToken при повторном обращении ИС Потребителя БДн не совпало с указанным ЕБС в полученном результате верификации:

Шаг 19а.1 При проверке ЕСИА возможности предоставления ИС-Потребителя БДн доступа к персональным данным значение verifyToken при повторном обращении ИС-Потребителя БДн не совпало с указанным ЕБС в полученном результате верификации.

Шаг 19а.2 ЕСИА возвращает ответ с сообщением об ошибке проведения усиленной аутентификации.

Шаг 19а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Исключительный сценарий 9 – Пользователь не подтвердил свое согласие на передачу персональных данных:

Шаг 21а.1 При запросе подтверждения Пользователем сервиса передачи персональных данных, ЕСИА получен отрицательный ответ.

Шаг 21а.2 ЕСИА возвращает ответ с сообщением об ошибке проведения усиленной аутентификации.

Шаг 21а.3 Пользователю выдается ошибка. Усиленная аутентификация не пройдена.

Завершение сценария

Список технологий и типов данных:

Приложение ДКО: WEB-приложение ИС-Потребителя БДн.

UI ЕБС: WEB-форма съема биометрии.

4 ОСНОВНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

4.1 Реализация процесса «Регистрация биометрических данных в ЕБС»

Взаимодействие Системы и ИС КО - Поставщиков БДн осуществляется через СМЭВ 3.х.

Применение СМЭВ на этапе биометрической регистрации предполагает возможность взаимодействия Системы с любыми ИС организаций, зарегистрированными в СМЭВ и имеющими право проводить полную биометрическую регистрацию.

4.1.1 Технические рекомендации к оборудованию для получение биометрических образцов в офисе кредитной организации

4.1.1.1 Требования к техническим характеристикам оборудования для регистрации изображения лица

Для регистрации изображения лица необходимо использовать фото или видеокамеру (далее - камеру) со следующими характеристиками:

- разрешение получаемого изображения: не менее 1280x720 пикселей;
- при расположении субъекта на расстоянии 0,3-0,5 м от камеры, эквивалентное фокусное расстояние должно составлять от 31 до 100 мм;
- при расположении субъекта на расстоянии 0,51-1,0 м от камеры, эквивалентное фокусное расстояние должно составлять от 28 мм до 100 мм от камеры;
- фото-видеосъемка должна проводится при использовании режима автоматической корректировки баланса белого цвета.

Для обеспечения естественной цветопередачи кожи рекомендуется, чтобы цветовая температура осветителей составляла от 4800 до 6500 К. Требуемая цветовая температура обеспечивается люминесцентными или светодиодными источниками освещения. Используемые источники освещения должны создавать в области лица освещенность:

- для видео/фотокамер без автоматической коррекции освещенности не менее 300 лк;
- для видео/фотокамер с автоматической коррекцией освещенности не менее 100 лк.

4.1.1.2 Требования к техническим характеристикам оборудования для регистрации записи голоса

Для регистрации записи голоса необходимо использовать микрофон со следующими характеристиками:

- тип: конденсаторный (предпочтительно электретный), без автоматической регулировки усиления;
- соотношение сигнал/шум: не менее 58 дБ;
- диапазон частот: от 40 до 10000 Гц;
- чувствительность: не менее минус 30 дБ;
- форма диаграммы направленности: всенаправленная, кардиоида, суперкардиоида или гиперкардиоида.

4.1.2 Рекомендации по организации процесса сбора биометрических данных в офисе кредитной организации

При сборе биометрических данных рекомендуется использовать веб-браузеры Mozilla FireFox, Apple Safari, версий, официально поддерживаемых производителями.

Рекомендуемый алгоритм сбора биометрических данных представлен на рисунке (см. Рисунок 4).

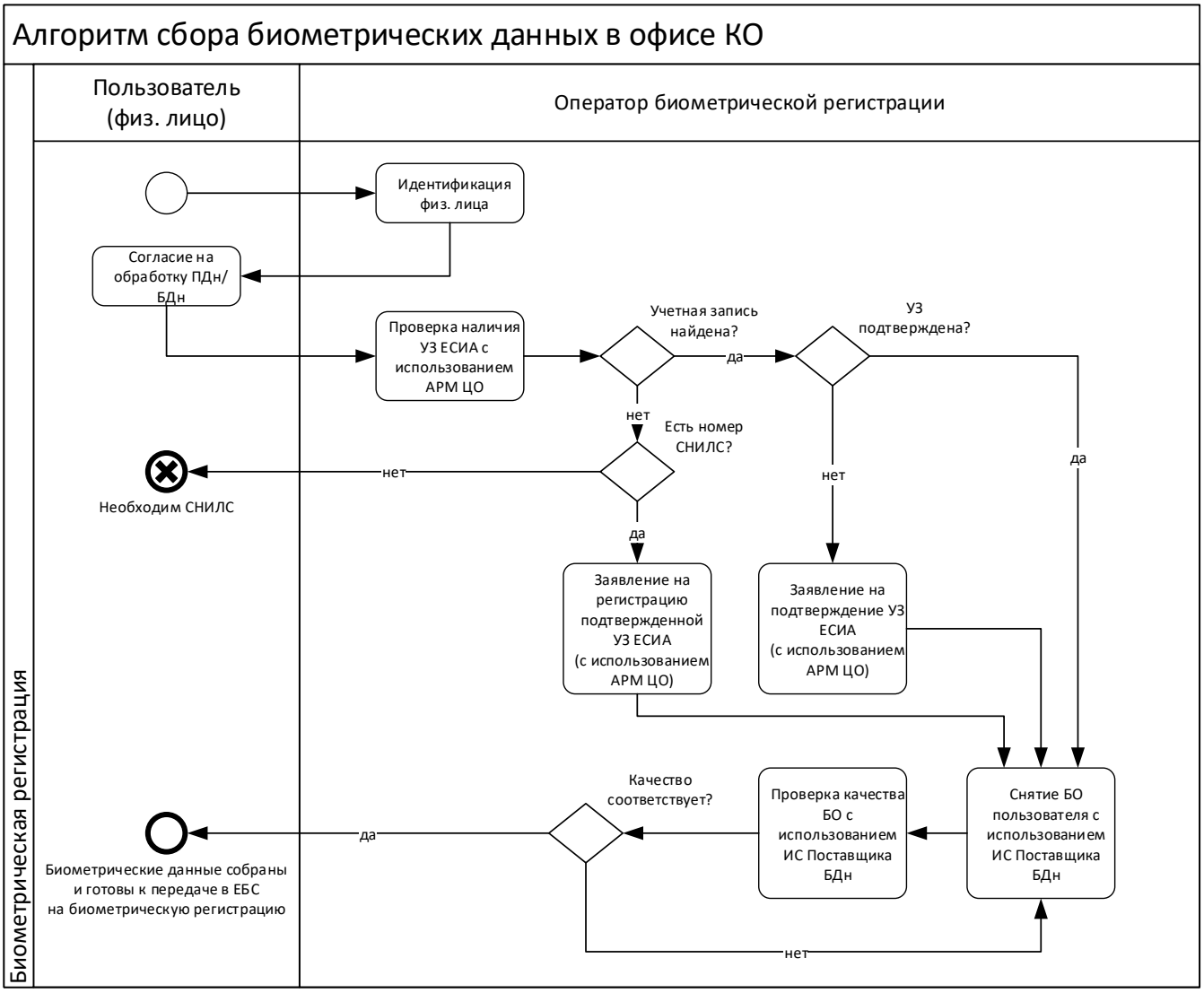

Рисунок 4 – Рекомендуемый алгоритм сбора биометрических данных в офисе КО

При использовании АРМ ЦО необходимо руководствоваться Руководством оператора центра обслуживания ЕСИА[3]. Вход в приложение АРМ ЦО осуществляется по ссылке: https://esia.gosuslugi.ru/ra/.

4.1.3 Требования к предоставляемым биометрическим образцам

Для проведения биометрической регистрации должны использоваться фотоизображение лица и аудиозапись голоса клиента.

4.1.3.1 Изображение лица

Фотоизображения лица должны соответствовать требованиям, установленным ГОСТ Р ИСО/МЭК 19794-5-2013 для полного фронтального типа изображения лица, в том числе:

[3] http://minsvyaz.ru/ru/documents/4247/

- цвета пикселей изображений фронтального типа должны быть представлены в 24-битовом цветовом пространстве RGB, в котором на каждый пиксель приходится по 8 битов на каждый компонент цвета: красный, зелёный и синий;
- поворот головы должен быть не более 5° от фронтального положения;
- наклон головы должен быть не более 5° от фронтального положения;
- отклонение головы должно быть не более 8° от фронтального положения;
- расстояние между центрами глаз должно составлять не менее 120 пикселей;
- при расстоянии между центрами глаз 120 пикселей рекомендуемое значение:
    - горизонтального размера изображения лица составляет 480 пикселей;
    - вертикального изображения лица составляет 640 пикселей;
- не допускается перекрытие волосами или посторонними предметами изображение лица по всей ширине от бровей до нижней губы;
- на изображении должно присутствовать только одно лицо, наличие других лиц, фрагментов других лиц и портретов не допускается;
- выражение лица должно быть нейтральным, рот закрыт, оба глаза открыты нормально для соответствующего субъекта (включая поведенческие факторы или медицинские заболевания);
- лицо должно быть равномерно освещено, чтобы на изображении лица отсутствовали тени и блики: отношение между средними интенсивностями квадратных областей вокруг контрольных точек 5.3 и 5.4 (см. Рисунок 5) с размером сторон, равным 20% расстояния между центрами глаз, должно быть между 0,5 и 2,0;
- не допускается использование ретуши и редактирования изображения;
- допускается кадрирование изображения;
- в случае фотографирования человека в очках не допускается наличие солнцезащитных очков и ярких световых артефактов или отражения вспышки от очков;
- изображение лица должно быть сохранено в файле .jpeg или .png.

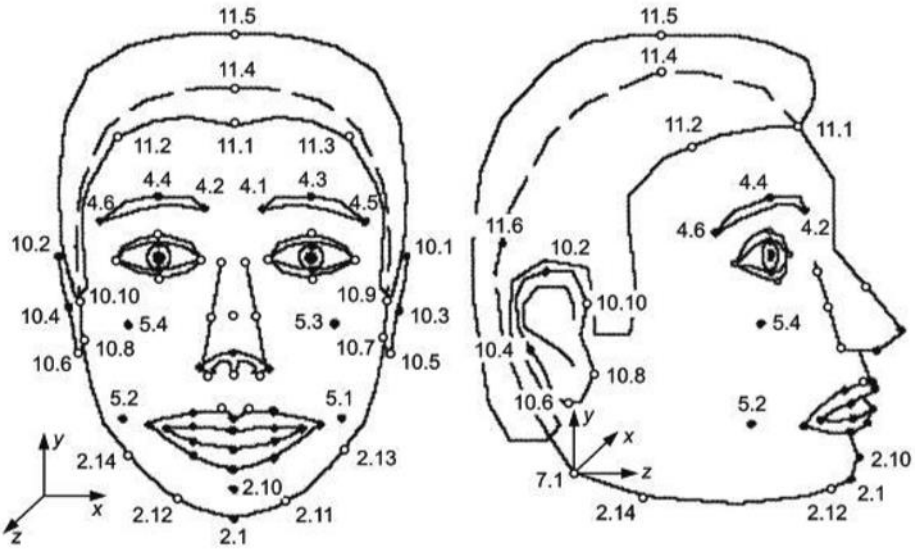

Рисунок 5 Коды контрольных точек лица

4.1.3.2 Запись голоса

БО записи голоса должны соответствовать следующим требованиям:

- отношение сигнал-шум для звука не менее 15 дБ;
- глубина квантования не менее 16 бит;
- частота дискретизации не менее 16 кГц;
- контейнер/формат: RIFF (WAV);
- код сжатия (Compression Code): PCM/uncompressed (0x0001);
- количество каналов в записи голоса: 1 (монорежим) канал;
- не допускается использовать шумоподавление;
- на записи должен присутствовать голос одного человека;
- запрещено получение БКШ путем перекодирования фонограмм, записанных с помощью технических средств телефонной сети общего пользования (ТфОП).

Для текстозависимого алгоритма распознавания по голосу:

- длительность записи голоса зависит от размера используемого словаря;
- содержание речи субъекта: парольная фраза;
- эмоционально-психологическое состояние и состояние здоровья субъекта: нормальное не возбужденное состояние без явных проявлений каких-либо заболеваний (простудные, респираторные и т.п.);

- перечень языков, на которых субъект может производить речевое сообщение: русский.

4.1.3.2.1 Рекомендации к произносимым последовательностям

При снятии биометрического образца записи голоса, Поставщик БДн может записать три образца голоса пользователя.

При записи первого образца голоса, пользователь должен произнести следующую фразу, состоящую из возрастающей последовательности цифр: 0 1 2 3 4 5 6 7 8 9.

При записи второго образца голоса, пользователь должен произнести следующую фразу, состоящую из убывающей последовательности цифр: 9 8 7 6 5 4 3 2 1 0.

При записи третьего образца голоса, пользователь должен произнести следующую фразу, состоящую из заданной последовательности цифр: 5 9 4 7 3 1 8 6 0 2.

ВНИМАНИЕ! Необходимо произносить фразы разборчиво. Числа необходимо произносить в соответствии со следующим правилом: 0 – ноль, 1 – один, 2 – два, 3 – три, 4 – четыре, 5 – пять, 6 – шесть, 7 – семь, 8 – восемь, 9 – девять, иное произношение чисел (например, «нуль», «раз», «двойка» и т.п.) не допускается. При произношении последовательности цифр не допускается их группировка (например, десятками, сотнями и т.п.).

В итоге, формируется один файл с записью голоса. Передаваемые метаданные должны содержать время начала и окончания записи каждого образца. При этом, значение времени рассчитывается в секундах от начала файла.

При формировании запроса на регистрацию биометрических образцов согласно Виду сведений «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию» версии 1.2.0 необходимо склеить записи образцов голоса в одну запись и заполнить поле BioMetadata с метаданными по записи голоса.

Для первого образца записи голоса, который содержит фразу, состоящую из возрастающей последовательности цифр, необходимо заполнить следующие поля:

```
<Key>voice_1_start</Key>
<Value>00.000</Value>
<Key>voice_1_end</Key>
<Value>10.002</Value>
```

```
<Key>voice_1_desc</Key>
<Value>digits_asc</Value>
```

Где voice_1_start содержит время начала записи первого образца, voice_1_end содержит время конца записи первого образца и voice_1_desc содержит идентификатор digits_asc, что данный образец содержит возрастающую последовательность цифр.

Для второго образца записи голоса, который содержит фразу, состоящую из убывающей последовательности цифр, необходимо заполнить следующие поля:

```
<Key>voice_2_start</Key>
<Value>12.601</Value>
<Key>voice_2_end</Key>
<Value>20.199</Value>
<Key>voice_2_desc</Key>
<Value>digits_desc</Value>
```

Где voice_2_start содержит время начала записи второго образца, voice_2_end содержит время конца записи второго образца и voice_2_desc содержит идентификатор digits_desc, что данный образец содержит убывающую последовательность цифр.

Для третьего образца записи голоса, который содержит фразу, состоящую из заданной последовательности цифр, необходимо заполнить следующие поля:

```
<Key>voice_3_start</Key>
<Value>22.001</Value>
<Key>voice_3_end</Key>
<Value>30.102</Value>
<Key>voice_3_desc</Key>
<Value>digits_random</Value>
```

Где voice_3_start содержит время начала записи третьего образца, voice_3_end содержит время конца записи третьего образца и voice_3_desc содержит идентификатор digits_random, что данный образец содержит заданную последовательность цифр.

4.1.4 Вид Сведений «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию»

Разработан Вид сведений (ВС), в соответствии с актуальной версией Методических рекомендаций по работе с Единой системой межведомственного электронного взаимодействия версии 3.x, опубликованной на технологическом портале СМЭВ (актуальная версия). ВС обеспечивает реализацию метода регистрации биометрических данных в Системе.

Описание разработанного Вида сведений расположено в Приложении А (см. ПРИЛОЖЕНИЕ А. Вид сведений в единой системе межведомственного электронного взаимодействия «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию»).

4.1.4.1 Передача метрик событий процесса биометрической регистрации

Для осуществления контроля процесса сбора параметров БДн (данные изображения лица, данные голоса) через систему мониторинга бизнес-процессов необходимо в виде сведений «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию» передавать значения событий, приведенных в таблице «Реестр событий» (см. Таблица 4).

Значения перечисленных событий в таблице «Реестр событий» должны фиксироваться только в автоматическом режиме. При отсутствии технической возможности фиксации времени возникновения или завершения описанных событий в таблице «Реестр событий», значение не передается в виде сведений «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию».

КО передает собранную информацию о событиях при вызове ВС ЕБС «Универсальный вид сведений для приема заявлений на биометрическую регистрацию» в блоке метаданных заявителя (тег "PersonMetadata").

```
<xs:complexType name="MetadataType">
    <xs:sequence>
        <xs:element name="Key" type="tns:string-50">
            <xs:annotation>
                <xs:documentation>Ключевое значение метаданных</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="Value" type="tns:string-500">
            <xs:annotation>
                <xs:documentation>Значение метаданных</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
</xs:complexType>
```

Не допускается повторение ключей значения метаданных PersonMetadata в рамках одного BiometricData.

Передача событий, произошедших после вызова ВС ЕБС, не требуется.

Пример заполнения:

```
<PersonMetadata>
    <Key>consent_time_start</Key>
```

```
    <Value>2018-11-28 14:30:27</Value>
    <Key>consent_time_end</Key>
    <Value>2018-11-28 14:35:48</Value>
</PersonMetadata>
```

4.1.4.1.1 Реестр событий

Тип данных, используемых в событиях:

- timestamp – дата и время события в формате YYYY-MM-DD HH:MM:SS.MsMsMs (пример "2018-11-28 14:53:27.000");
- messageId – идентификатор в формате строки (string) (пример "8559d279-3133-11e9-81b9-fa163ea6d066");
- string – строка, не пустая. (пример {"code": 108, "version": { "library": "1.0.8.0", "configuration": "v1", "service": "1.0.8.9" }, "metadata": { "length": { "value": 381.000, "state": "passed" }, "sample_rate": { "value": 8000.000, "state": "failed" }, "channels": { "value": 1.000, "state": "passed" }, "depth": { "value": 16.000, "state": "passed" }, "duration": { "value": 24.000, "state": "passed" } }}).

<part> - номер попытки в рамках одной сессии биометрической регистрации (в рамках одного BiometricData), целые числа начиная с 1.

Таблица 4. Реестр событий

№	Событие	Мнемоника	Value (type)	Обязательное	Комментарий
1	Начало процесса обслуживания Клиента по операции регистрации биометрических образцов в ЕБС.	total_reg_time_start	timestamp	Обязательное	Первичный запрос на поиск Клиента в системе Банка (АБС).
2	Завершение процесса обслуживания гражданина РФ в ЦО КО Завершение процесса обслуживания Клиента по операции регистрации	total_reg_time_end	timestamp	Обязательное	Время завершения процесса обслуживания Клиента по операции регистрации БО в ЕБС.

№	Событие	Мнемоника	Value (type)	Обязательное	Комментарий
	биометрических образцов в ЕБС.				
3	Начало процесса приёма нового клиента на обслуживание в КО	new_client_time_start	timestamp	Необязательное	Событие при входе в бизнес-процесс создания нового Клиента в системе Банка (АБС), в случае если Клиент не был найден.
4	Завершение процесса приёма нового клиента на обслуживание в КО	new_client_time_end	timestamp	Необязательное	Событие при успешной идентификации Клиента (открытие идентификационной сессии) после создания нового Клиента в системе Банка (АБС).
5	Передача оператором ЦО КО клиенту формы согласия	consent_time_start	timestamp	Обязательное	Печать формы согласия из ИС КО для передачи на подпись клиенту или на шаге бизнес-процесса, при котором Клиенту передается согласие на подписание (в случае, если печати нет).
6	Получение оператором ЦО КО подписанной клиентом формы согласия	consent_time_end	timestamp	Обязательное	**Опционально**. Заполняется, в случае, если бизнес-процесс позволяет зафиксировать событие получения подписанного согласия от Клиента (переход на следующую форму с формы печати согласия, выставление признака получения согласия). При отсутствии возможности определения timestamp события, передавать <Value>2000-01-01 00:00:00.000</Value>
7	Инициирование оператором ЦО КО начало съема лица клиента. Для каждой попытки.	photo_time_start_<part>	timestamp	Обязательное	Дата и время, когда уполномоченный сотрудник ЦО КО инициировал в АРМ начала съема лица клиента. Для каждой попытки, последовательно.
8	Завершение проверки качества, собранного БО изображения лица клиента. Для каждой попытки.	photo_time_end_<part>	timestamp	Обязательное	Дата и время завершения проверки качества, собранного БО изображения лица на соответствие требованиям с использованием ПО контроля качества за успешную попытку. Для каждой попытки, последовательно.

№	Событие	Мнемоника	Value (type)	Обязательное	Комментарий
9	Показатели, возвращаемые БКК по результатам проверки БО изображения лица. Для каждой попытки.	front_bqc_estimators_photo_<part>	string	Обязательное	Строка, передаваемая в АРМ библиотекой контроля качества со значениями результатов проверки качества БО изображения лица. Для каждой попытки, последовательно.
10	Инициирование оператором ЦО КО начала записи первого БО записи голоса Клиента. Для каждой попытки.	sound_direct_time_start_<part>	timestamp	Обязательное	Дата и время, когда уполномоченный сотрудник ЦО КО инициировал в АРМ начало записи для произнесения первой последовательности цифр, расположенных в порядке возрастания. Для каждой попытки, последовательно.
11	Завершение проверки первого БО записи голоса. Для каждой попытки.	sound_direct_time_end_<part>	timestamp	Обязательное	Дата и время завершения проверки качества первого собранного БО записи голоса на соответствие требованиям с использованием ПО контроля качества. Для каждой попытки, последовательно.
12	Показатели возвращаемые БКК по результатам проверки первого собранного БО записи голоса. Для каждой попытки.	front_bqc_estimators_sound_direct_<part>	string	Обязательное	Строка, передаваемая в АРМ библиотекой контроля качества со значениями результатов проверки качества БО записи голоса. Для каждой попытки, последовательно.
13	Инициирование оператором ЦО КО начала записи второго БО записи голоса. Для каждой попытки.	sound_reverse_time_start_<part>	timestamp	Обязательное	Дата и время, когда уполномоченный сотрудник ЦО КО инициировал в АРМ начало записи для произнесения второй последовательности цифр, расположенных в порядке убывания. Для каждой попытки, последовательно.
14	Завершение проверки второго собранного БО записи голоса. Для каждой попытки.	sound_reverse_time_end_<part>	timestamp	Обязательное	Дата и время завершения проверки качества второго собранного БО записи голоса на соответствие требованиям с использованием ПО контроля качества. Для каждой попытки, последовательно.

№	Событие	Мнемоника	Value (type)	Обязательное	Комментарий
15	Показатели возвращаемые БКК по результатам проверки БО второй записи голоса. Для каждой попытки.	front_bqc_estimators_sound_reverse_<part>	string	Обязательное	Строка, передаваемая в АРМ библиотекой контроля качества со значениями результатов проверки качества БО записи голоса. Для каждой попытки, последовательно.
16	Инициирование оператором ЦО КО начала записи третьего БО записи голоса. Для каждой попытки.	sound_random_time_start_<part>	timestamp	Обязательное	Дата и время, когда уполномоченный сотрудник ЦО КО инициировал в АРМ начало записи для произнесения третьей последовательности цифр, расположенных в заданном порядке. Для каждой попытки, последовательно.
17	Завершение проверки третьего собранного БО записи голоса. Для каждой попытки.	sound_random_time_end_<part>	timestamp	Обязательное	Дата и время завершения проверки качества третьего собранного БО записи голоса на соответствие требованиям с использованием ПО контроля качества. Для каждой попытки, последовательно.
18	Показатели возвращаемые БКК по результатам проверки БО третьей записи голоса. Для каждой попытки.	front_bqc_estimators_sound_random_<part>	string	Обязательное	Строка, передаваемая в АРМ библиотекой контроля качества со значениями результатов проверки качества БО записи голоса. Для каждой попытки, последовательно.
19	Завершение проверки записи, склеенной в одну запись. Для каждой попытки.	sound_all_time_end_<part>	timestamp	Обязательное	Дата и время завершения проверки записи, склеенной в одну запись, на соответствие требованиям с использованием ПО контроля качества. Для каждой попытки, последовательно.
20	Показатели возвращаемые БКК по результатам проверки БО склеенной записи голоса. Для каждой попытки.	front_bqc_estimators_sound_all_<part>	string	Обязательное	Строка, передаваемая в АРМ библиотекой контроля качества со значениями результатов проверки качества БО записи голоса. Для каждой попытки, последовательно.
21	Инициирование оператором ЦО КО начала поиска УЗ клиента в ЕСИА.	bank_find_profile_time_start_<part>	timestamp	Обязательное	Дата и время, когда уполномоченный сотрудник ЦО КО инициировал отправку запроса по поиску учётной

№	Событие	Мнемоника	Value (type)	Обязательное	Комментарий
	Для каждой попытки.				записи клиента в ЕСИА. Для каждой попытки.
22	Получение ИС КО ответа на запрос по поиску УЗ клиента в ЕСИА. Для каждой попытки.	bank_find_profile_time_end_<part>	timestamp	Обязательное	Дата и время, когда ИС КО подтвердило приём сообщения от СМЭВ, содержащего ответ на запрос по поиску учётной записи в ЕСИА. Для каждой попытки.
23	Запрос в ЕСИА на поиск УЗ.	esia_find_account_msg_id	string	Обязательное	Идентификатор запроса на поиск УЗ в ЕСИА
24	Запрос ВС "Подтверждение личности гражданина РФ или иностранного гражданина в ЕСИА".	esia_confirm_msg_id	messageId	Необязательное	Идентификатор запроса, направленного на подтверждение личности клиента, УЗ которого находится в одном из статусов: • упрощенная, готовая к подтверждению; • стандартная; • подтвержденная через ФГУП «Почта России»
25	Запрос ВС "Подтверждение учётной записи в ЕСИА, созданной на основе существующей упрощённой".	esia_register_by_simplified_msg_id	messageId	Необязательное	Идентификатор запроса, направленного на подтверждение УЗ клиента КО в ЕСИА, имеющей статус «Упрощенная»
26	Идентификатор запроса обновления УЗ клиента в ЕСИА.	esia_recover_msg_id	string	Необязательное	Идентификатор запроса обновления УЗ клиента в ЕСИА
27	Наименование оборудования (камера)	name_equipment_camera	string	Обязательное	
28	Наименование оборудования (микрофон)	name_equipment_microphone	string	Обязательное	

4.1.5 Библиотека контроля качества

В целях обеспечения проверки качества снимаемых БО в процессе биометрической регистрации, необходимо использовать предоставляемую ЕБС библиотеку контроля качества,

интегрируемую в ИС КО - Поставщика БДн. Получить библиотеку контроля качества (далее БКК) можно на доступном интернет ресурсе[4].

БКК используется для контроля качества собранных биометрических образцов только в целях регистрации БДн граждан в ЕБС. Дополнительная доработка и настройка БКК на стороне Поставщика БДн не требуется.

4.2 Реализация процесса «Удаленная идентификация с использованием биометрической верификации ЕБС»

Взаимодействие Системы и ИС КО - Потребителей БДн осуществляется через взаимодействие с ЕСИА посредством API биометрической верификации.

API биометрической верификации имеет возможность взаимодействия с любыми ИС Участников биометрического взаимодействия – Потребителей БДн.

Общее описание API биометрической верификации приведено в разделе 4.2.2. Детальное описание API биометрической верификации приведено в Приложении Б (см. ПРИЛОЖЕНИЕ Б. Описание интеграции внешних систем с Единой биометрической системой в процессе биометрической верификации).

4.2.1 Общая схема взаимодействия при удалённой идентификации

Взаимодействие систем при удалённой идентификации осуществляется в несколько этапов:

1. Этап 1. Инициация удалённой идентификации.
2. Этап 2. Получение специального маркера доступа для взаимодействия с ЕБС.
3. Этап 3. Биометрическая верификация пользователя в ЕБС.
4. Этап 4. Завершение удалённой идентификации пользователя в ЕСИА/ЕБС.
5. Этап 5. Пользователь удалённо идентифицирован в ЕСИА/ЕБС.

[4] https://bio.rt.ru/documents/software/

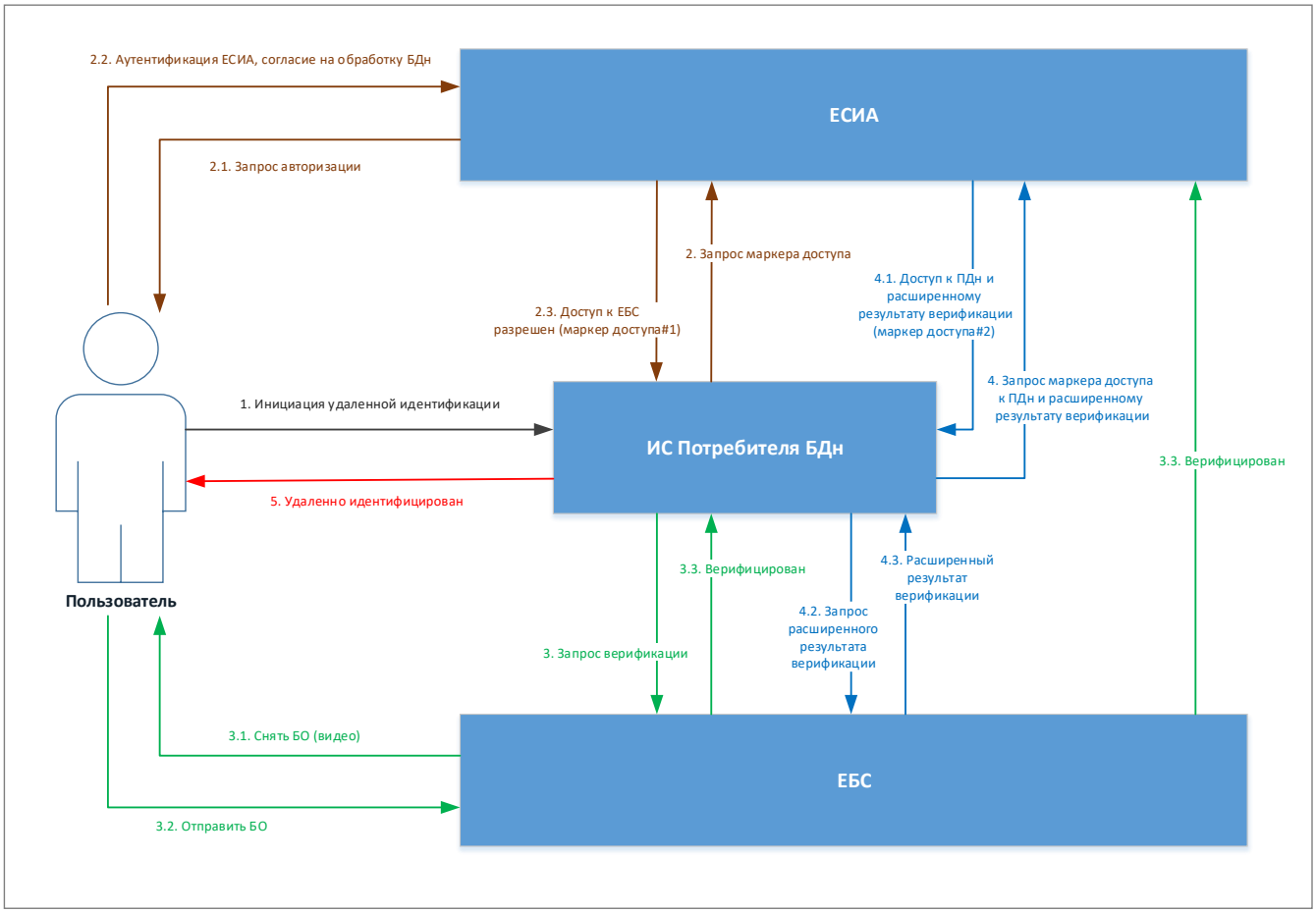

Рисунок 6 – Общая схема взаимодействия при удалённой идентификации

Этап 1. Инициация удаленной идентификации

Инициация процедуры происходит при выборе Пользователем услуги в ДКО КО (web или мобильное приложение), предоставляемой кредитной организацией и оказание которой предусматривает прохождение процедуры удаленной идентификации.

Реализация взаимодействия ИС Потребителя БДн с ЕСИА при инициации удаленной идентификации производится согласно актуальной версии Методических рекомендаций по использованию Единой системы идентификации и аутентификации (далее «МР ЕСИА»), в частности:

- Раздел 3 «Аутентификация пользователей через ЕСИА»;
- Раздел 3.4 «Требования к визуальному оформлению входа посредством ЕСИА»;
- Раздел 3.1.2 «Аутентификация с использованием OpenID Connect 1.0»;

– Приложения Б и В.

Для доступа к сервису авторизации продуктивной ЕСИА должны использоваться каналы взаимодействия и адреса, указанные в разделе 8 Приложения Б.

Этап 2. Получение специального маркера доступа для взаимодействия с ЕБС

В случае использования в качестве ДКО web-приложения, ИС Потребителя БДн реализует в ДКО, согласно 3 шага раздела 3.1.2 МР ЕСИА, аутентификацию клиента и получение специального маркера доступа для взаимодействия с ЕБС, разрешающего клиенту биометрическую верификацию в ЕБС. Для этого Потребитель БДн реализует взаимодействие с сервисом авторизации и получения маркера доступа ЕСИА, согласно Приложения В.2 «Модель контроля на основе делегированного принятия решения» МР ЕСИА.

В запросе на авторизацию ИС Потребителя БДн должна указать scope «openid» и специальный scope «bio».

Пользователь авторизуется в ЕСИА по логину и паролю и дает согласие на проведение усиленной аутентификации с использованием его биометрических данных в ЕБС (в случаях, если согласие пользователя из данной ИС-Потребителя БДн еще не получено). После авторизации пользователя в ЕСИА, ИС Потребителя БДн получит разрешение на доступ в виде авторизационнного кода. Данный авторизационный код ИС Потребителя БДн предъявляет ЕСИА при запросе маркера доступа (accessToken).

В случае использования в качестве ДКО мобильного приложения, Потребитель БДн встраивает в своё мобильное приложение SDK ЕБС (далее – SDK) для взаимодействия с МП ЕБС. При этом реализация взаимодействия ИС Потребителя БДн с ЕСИА происходит с участием МП ЕБС (см. Таблица 2, Основной сценарий, Шаг 1 – Шаг 11).

В результате завершения этапа, ИС Потребителя БДн получит специальный первичный маркер доступа (accessToken), обладающий следующими отличиями от стандартного маркера доступа ЕСИА:

– короткое время жизни (TTL);
– наличие в составе маркера доступа:

- URL REST-сервиса ЕСИА для передачи расширенного результата биометрической верификации из ЕБС;
- verifyToken и время прекращения действия результата биометрической верификации пользователя в ЕСИА (после указанного в параметре момента времени получение специального вторичного маркера доступа со скоупом ext_auth_result в ЕСИА будет невозможно).

Для инициации следующего этапа ИС Потребителя БДн вызывает метод «Старт верификации в ЕБС» REST-сервиса ЕБС.

Этап 3. Биометрическая верификация пользователя в ЕБС

ИС Потребителя БДн вызывает метод «Старт верификации в ЕБС» REST-сервиса ЕБС, в параметрах вызова необходимо передать:

- специальный маркер доступа (accessToken), полученный от ЕСИА на Этапе 2;
- redirect, содержащий URL, на который ЕБС должна перенаправить Пользователя после проведения биометрической верификации.

ЕБС проверяет:

- параметры специального маркера доступа (валидация ЭП ЕСИА, сроки действия);
- права ИС Потребителя БДн использовать сервис верификации ЕБС (авторизация ИС Потребителя БДн);
- наличие в ЕБС активного БКШ Пользователя, по предоставленному в маркере доступа OID УЗ Пользователя ЕСИА.

В ответ на вызов, ЕБС возвращает сообщение по протоколу HTTP (код состояния 302 (для API версии v1) или 200 (для API версии v2)), содержащее идентификатор сессии верификации ЕБС и адрес WEB-формы ЕБС для получения БО.

Дальнейший процесс различается для случаев используемого канала ДБО:

- в случае использования WEB-приложения Потребителя БДн, снятие БО производит WEB-форма ЕБС;
- в случае использования МП Потребителя БДн, снятие БО производит МП ЕБС.

При использовании WEB-приложения Потребителя БДн:

1. ИС Потребителя БДн перенаправляет браузер пользователя на WEB-форму ЕБС съема БО (URL WEB-формы ЕБС съема БО, на который необходимо осуществить перенаправление пользователя для снятия биометрических образцов содержится в HTTP заголовке «Location» в случае успешного ответа метода «Старт верификации в ЕБС», (см. ПРИЛОЖЕНИЕ Б. Описание интеграции внешних систем с Единой биометрической системой в процессе биометрической верификации).
2. Вызванная WEB-форма ЕБС съема БО отображает пользователю инструкцию с описанием действий по формированию биометрических образцов.
3. Пользователь выполняет предлагаемые действия в процессе записи видеоизображения.
4. ЕБС проводит биометрическую верификацию.
5. При положительном результате биометрической верификации ЕБС перенаправляет браузер пользователя на URL, ранее указанный ИС Потребителем БДн в параметре redirect. ЕБС использует значение URL ИС Потребителя БДн, переданное в параметре «redirect» при вызове метода «Старт верификации в ЕБС», перенаправление содержит параметры verifyToken[5] и expired[6] (см. ПРИЛОЖЕНИЕ Б. Описание интеграции внешних систем с Единой биометрической системой в процессе биометрической верификации, п. 5.2 и 6.2). В случае получения ошибки, WEB-форма предлагает пользователю вернуться в Банк (кнопка «Назад в банк», по нажатию на которую, WEB-форма перенаправляет пользователя на ИС Потребителя БДн по ссылке, содержащейся в параметре «redirect»).

При использовании мобильного приложения МП Потребителя БДн и МП ЕБС:

1. ИС Потребителя БДн извлекает из сообщения HTTP Redirect ЕБС идентификатор сессии и передает его в МП ЕБС;
2. МП ЕБС вызывает метод «Согласование методов сбора БО и Liveness» REST-сервиса ЕБС и получает от ЕБС требуемые инструкции с описанием действий по формированию биометрических образцов;

[5] контрольное значение, необходимое для завершения процедуры аутентификации в ЕСИА после получения результата верификации.
[6] время прекращения действия результата биометрической верификации пользователя в ЕСИА, в миллисекундах с 1 января 1970 г. 00:00:00 GMT (после указанного в параметре момента времени получение специального маркера доступа со скоупом ext_auth_result в ЕСИА будет невозможно)

3. МП ЕБС отображает Пользователю интерфейс съема биометрии;
4. Пользователь выполняет предлагаемые действия в процессе записи видеоизображения;
5. МП ЕБС вызывает метод «Приём БО на верификацию» REST-сервиса ЕБС, передаёт сформированные БО (видеофайл) и получает в ответном сообщении результат, содержащий параметры verifyToken и expired;
6. МП ЕБС возвращает в МП Потребителя БДн параметры verifyToken и expired как результат успешной верификации в ЕБС. В случае получения ошибки, МП ЕБС возвращает в МП Потребителя БДн код «resultCode» и объект с пустыми полями verifyToken и expired (см. ПРИЛОЖЕНИЕ Г. Руководство пользователя по работе с библиотекой ЕБС.Sdk).

Этап 4. Завершение удаленной идентификации пользователя в ЕСИА/ЕБС

ИС Потребителя БДн реализует взаимодействие с сервисом авторизации и получения маркера доступа ЕСИА (аналогично Этапу 2)[7].

В запросе на авторизацию ИС Потребителя БДн должна указать scope «openid» и специальный scope «ext_auth_result[8]», параметр verifyToken, полученный на Этапе 3.

В результате, ИС Потребителя БДн получит специальный вторичный маркер доступа (accessToken). Данный маркер доступа ИС Потребителя БДн передает в составе запроса:

- в ЕСИА при запросе ПДн пользователя[9];
- в ЕБС при запросе получения расширенного результата верификации (см. Этап 5).

ЕСИА выдаст данный маркер доступа только в случае:

- наличия в ЕСИА успешного результата биометрической верификации Пользователя;

[7] для доступа к сервису авторизации продуктивной ЕСИА должны использоваться каналы взаимодействия и адреса, указанные в разделе 0 Приложения Б.
[8] данный scope дает возможность получения следующих данных: ФИО, пол, гражданство, дата рождения, реквизиты документа, удостоверяющего личность, адрес места жительства (регистрации) или места пребывания, место рождения, ИНН, СНИЛС, мобильный телефон, адрес электронной почты
[9] для доступа к сервису получения персональных данных продуктивной ЕСИА должны использоваться каналы взаимодействия и адреса, указанные в разделе 8 Приложения Б.

- успешного сравнения полученных параметров verifyToken от ЕБС и ИС-Потребителя БДн;
- если срок жизни параметра verifyToken не истёк: текущее время меньше, чем момент времени, указанный в параметре expired;
- наличия согласия Пользователя на предоставление персональных данных.

Пользователь автоматически аутентифицируется в ЕСИА.

Этап 5. Пользователь удаленно идентифицирован в ЕСИА/ЕБС успешно

ИС Потребителя БДн вызывает метод «Получение результата верификации» REST–сервиса ЕБС для получения расширенного результата биометрической верификации. В параметрах вызова необходимо передать специальный вторичный маркер доступа (accessToken), полученный от ЕСИА на Этапе 4.

В результате ИС Потребителя БДн получит расширенный результат верификации, который: содержит результат вычисления из единицы суммарной вероятности ложного совпадения и вероятности ложного совпадения по каждой биометрической модальности.

На основании полученного расширенного результата биометрической верификации, Потребитель БДн принимает решение о достаточности значений степеней схожести для оказания пользователю запрашиваемой услуги и перенаправляет пользователя на WEB-форму Потребителя БДн при использовании WEB-верификации, или на МП Потребителя БДн при использовании МП.

4.2.2 API биометрической верификации

4.2.2.1 Общее описание

Для обеспечения процесса биометрической верификации, в том числе взаимодействия ИС Потребителя БДн с ЕБС, реализован универсальный механизм API биометрической верификации ЕБС (см. ПРИЛОЖЕНИЕ Б. Описание интеграции внешних систем с Единой биометрической системой в процессе биометрической верификации).

Взаимодействие внешних систем с ЕБС посредством API биометрической верификации представлено на рисунках ниже (см. Рисунок 2 и Рисунок 3).

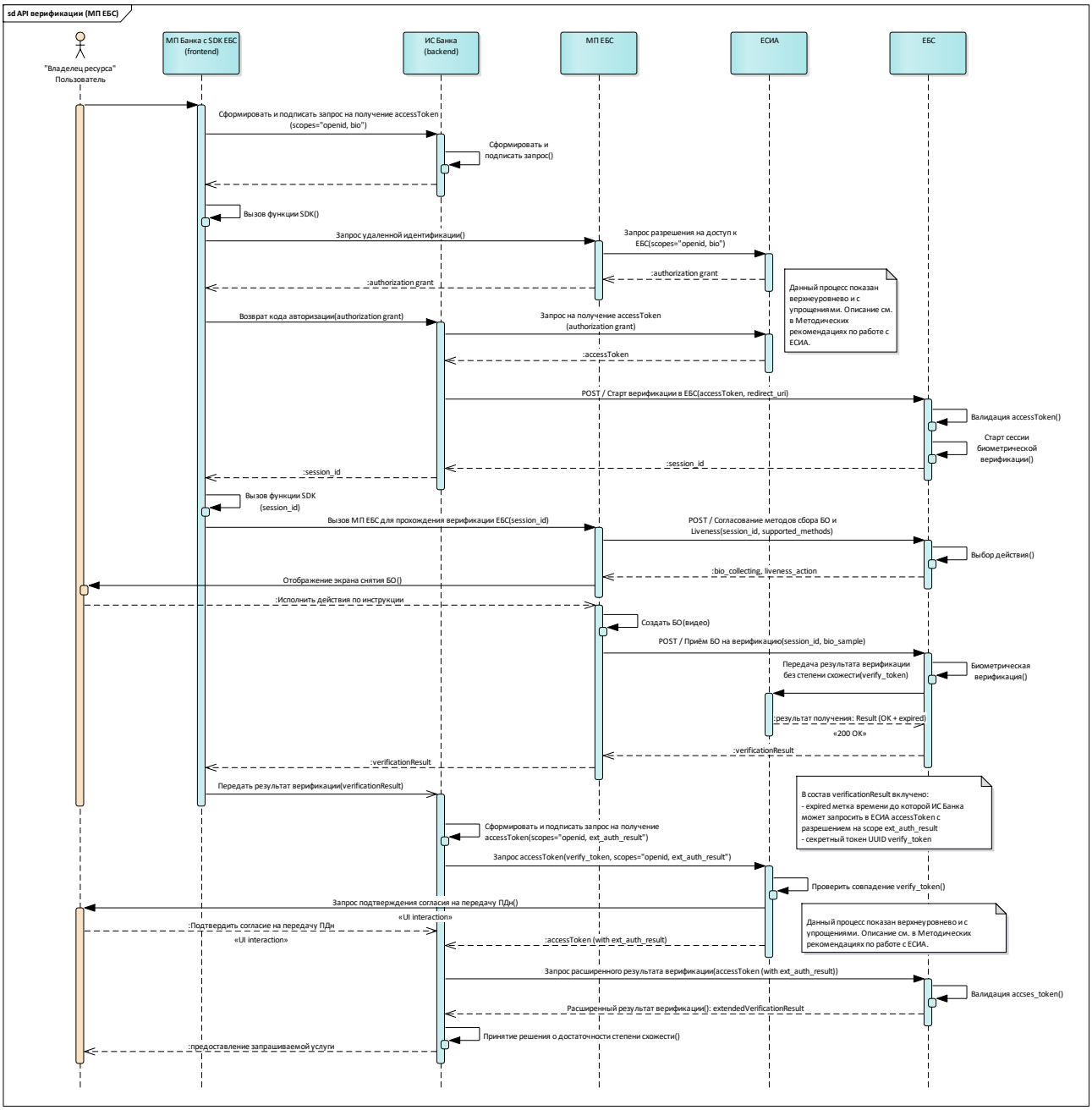

Рисунок 7 – Диаграмма последовательности API биометрической верификации с использованием в качестве ДКО мобильного приложения

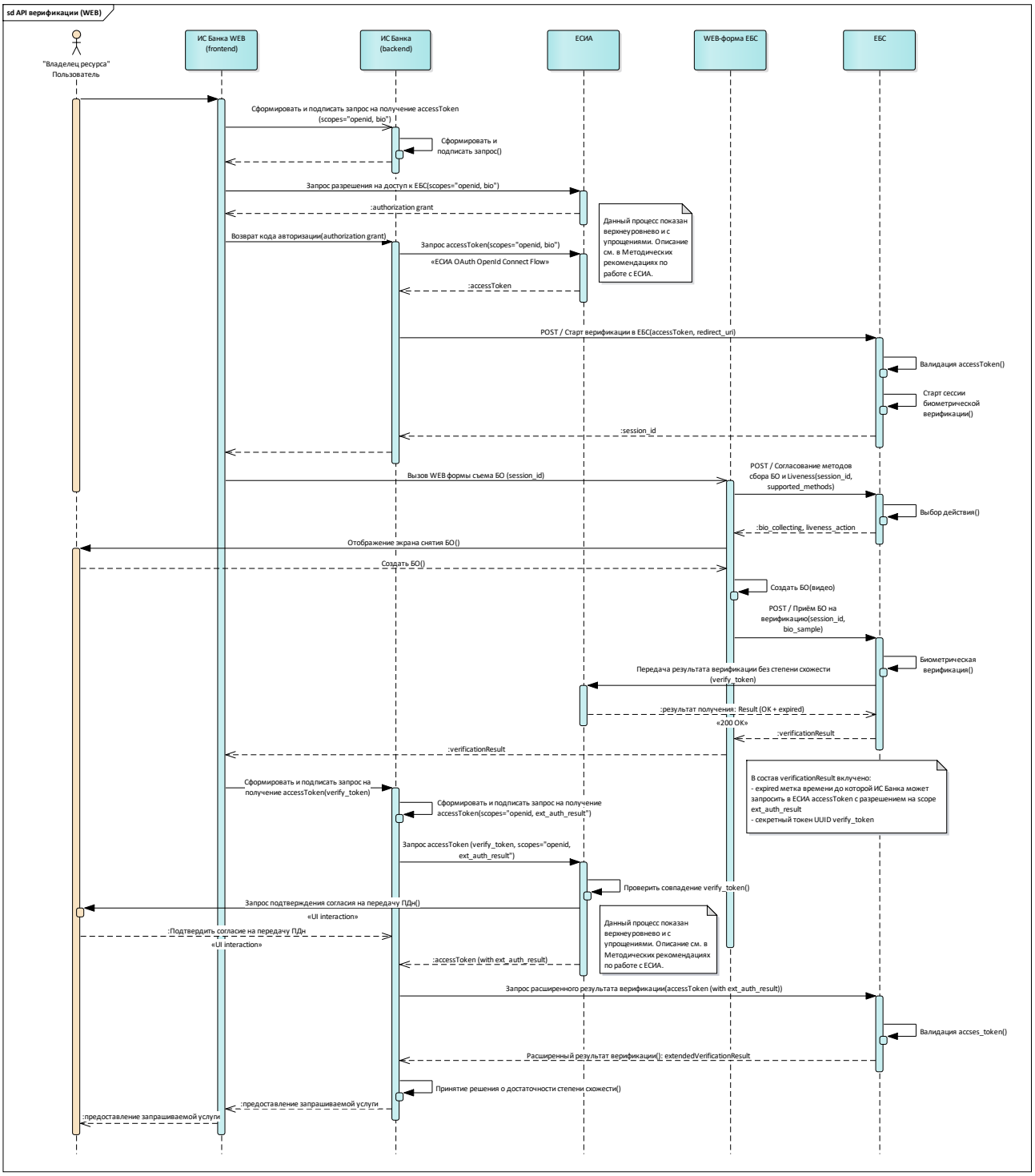

Рисунок 8 – Диаграмма последовательности API биометрической верификации с использованием в качестве ДКО WEB-приложения

4.2.3 Требования к мобильному приложению Потребителя БДн (интеграция SDK)

В целях обеспечения процесса удаленной идентификации с использованием в качестве ДКО мобильного приложения, Потребитель БДн должен интегрировать в своё мобильное

приложение SDK ЕБС (далее – SDK) для взаимодействия с МП ЕБС (см. ПРИЛОЖЕНИЕ Г. Руководство пользователя по работе с библиотекой ЕБС.Sdk).

SDK ЕБС обеспечивает:

1. Проверку наличия мобильного приложения для удаленной идентификации (МП ЕБС).
2. Взаимодействие МП Потребителя БДн и МП ЕБС для биометрической верификации.

Получить SDK для интеграции в МП Потребителя БДн можно на доступном интернет ресурсе[10].

Дополнительная доработка и настройка SDK на стороне Потребителя БДн не требуется.

Для прохождения удаленной идентификации, на мобильном устройстве Пользователя должно быть:

- установлено МП Потребителя БДн с интегрированной SDK ЕБС;
- установлено МП ЕБС;
- произведена первичная настройка МП ЕБС.

Взаимодействие МП Потребителя БДн со смежными приложениями и системами продемонстрировано на схеме ниже (см. Рисунок 9).

Описание установки и настройки МП ЕБС приведено в Приложении В (см. ПРИЛОЖЕНИЕ В. Описание установки и настройки мобильного приложения на ОС Android).

[10] https://bio.rt.ru/documents/software/

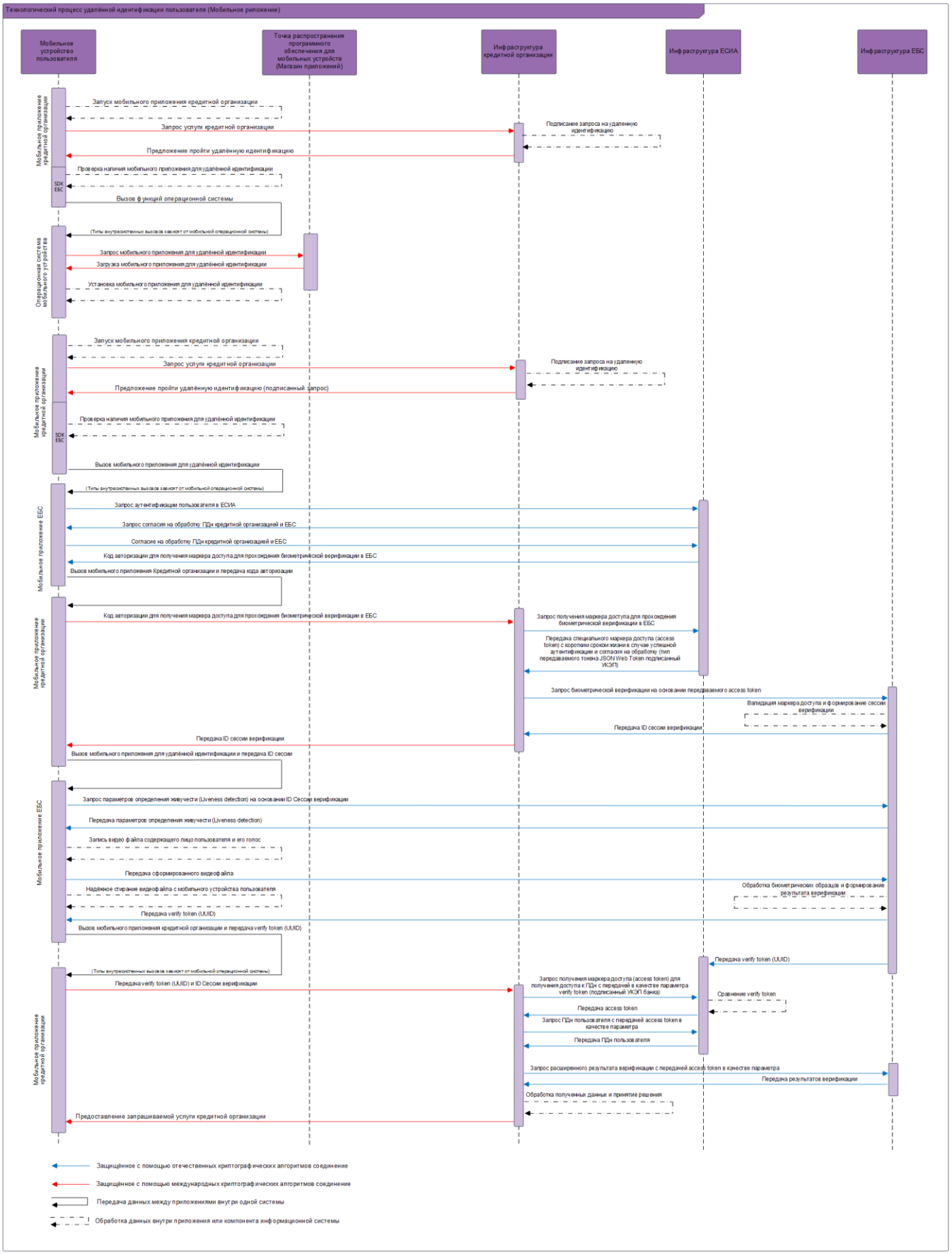

Рисунок 9 Эскиз технологической схемы процесса удалённой идентификации с использованием мобильного устройства

5 ТРЕБОВАНИЯ ДЛЯ ИНИЦИАЦИИ ПРОЦЕДУРЫ ПОДКЛЮЧЕНИЯ К ЕБС

5.1 Регистрация Поставщика БДн

Список авторизованных Поставщиков БДн формируется на основании нормативно-правовой документации[11]. Только авторизованный Поставщик БДн имеет право осуществить регистрацию в ЕБС. Для регистрации кредитной организации в ЕБС в качестве Поставщика БДн необходимо выполнить следующие обязательные условия:

1. Подключение и регистрация в тестовом контуре СМЭВ 3.xx в соответствии с разделом 10.6.2 «Регистрация Участника и/или информационной системы в тестовой среде» приложения 3 Правила и процедуры работы в СМЭВ по Методическим рекомендациям версии 3.x[12].
2. Подключиться к СМЭВ 3.xx и получить доступ к Универсальному Виду Сведений для приема заявлений на биометрическую регистрацию в продуктивном контуре СМЭВ 3.xx в соответствии с актуальными методическими рекомендациями и руководством пользователя ВС, схемами и контрольными примерами[13].
3. Получить доступ к сервису регистрации ЕСИА в соответствии с методическими рекомендациями ЕСИА, приложение «Г.1 Получение доступа к электронному сервису»[14].
4. В целях получения ID УЗ Пользователя ЕСИА и передаче его в ЕБС на этапе биометрической регистрации, Участник БВ должен получить статус «Оператор ЦО» в соответствии с Руководством оператора центра обслуживания ЕСИА[15]
5. Подготовить заявку и направить её Оператору ЕБС для согласования подключения к ЕБС, в соответствии с Правилами и процедурами взаимодействия Участников биометрического взаимодействия
6. В целях биометрической регистрации необходимо разработать приложение по съёму биометрических данных. В приложении должна использоваться SDK библиотеки контроля качества БДн, которую предоставляет Оператор ЕБС;
7. Выполнить процедуры подключения ИС в соответствии с Правилами и процедурами взаимодействия Участников биометрического взаимодействия.

[11] нормативно-правовые акты - https://bio.rt.ru/documents/npa/, перечень представлен по постоянной ссылке - https://www.cbr.ru/fintech/remote_authentication/
[12] постоянная ссылка - https://smev3.gosuslugi.ru/portal/
[13] постоянная ссылка - https://smev3.gosuslugi.ru/portal/
[14] актуальная версия методических рекомендаций ЕСИА опубликованы на портале Федерального Ситуационного центра Электронного Правительства https://minsvyaz.ru/documents/
[15] постоянная ссылка - http://minsvyaz.ru/ru/documents/4247/

При подключении к СМЭВ 3.xx необходимо пройти все процедуры в соответствии с правилами, опубликованными на портале https://smev3.gosuslugi.ru/portal/.

При подключении к ЕСИА необходимо пройти все процедуры в соответствии с регламентом, опубликованным на портале https://minsvyaz.ru/documents/.

При подключении к ЕБС необходимо пройти все процедуры в соответствии с Правилами и процедурами взаимодействия Участников биометрического взаимодействия.

Обязательное условие подключения Поставщика БДн, это успешное прохождение тестирования в интеграционной среде ЕБС. Успешное завершение тестирования должно быть подтверждено путём получения соответствующего уведомления от ЕБС.

5.1.1 Этапы настройки ИС Банка – Поставщика БДн

Для реализации взаимодействия ИС Банка с ЕБС необходимо осуществить следующие обязательные настройки:

- Осуществить получение усиленной квалифицированной подписи. Должны использоваться сертификаты ключей подписей, изготовленные аккредитованными Минкомсвязью России удостоверяющими центрами[16]. Структура сертификата ключа ЭП-ОВ должна соответствовать Требованиям к единой структуре сертификата ключа проверки электронной подписи, утверждаемым Приказом Федеральной службы безопасности РФ от 27.12.2011г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» и методическими рекомендациями от 14.02.2019 года №4-МР «Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, и проверке и передаче информации о степени соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации»;
- Осуществить организацию защищенного канала связи до СМЭВ в соответствии с разделом 10.10.1, 10.10.2 и 11.5 Приложение 3 Правила и процедуры работы в СМЭВ по Методическим рекомендациям версии 3.x[17];

[16] актуальный список представлен по постоянной ссылке - http://e-trust.gosuslugi.ru/CA
[17] постоянная ссылка - https://smev3.gosuslugi.ru/portal/

- Осуществить настройку оборудования со стороны Банка в соответствии с разделом 4.1.1 настоящего документа (для оборудования, осуществляющего сбор биометрических образцов) и Приложением 4 Требования к сети передачи данных участников информационного обмена[18] Особое внимание стоит обратить на возможные пути реализации банками требований к защите информации по классу КВ2:
  - самостоятельное проектирование и внедрение HSM и СПО для подписи банками, на основании Указания Банка России и ПАО «Ростелеком» от 09.07.2018 № 4859-У/01/01/782-18;
  - Использование типового решения по информационной безопасности. Для этого осуществить настройку типового решения по информационной безопасности в соответствии с Руководством программиста (см. ПРИЛОЖЕНИЕ Д. Руководство программиста по типовому решению информационной безопасности) и Руководством администратора (см. ПРИЛОЖЕНИЕ Е. Руководство администратора по типовому решению информационной безопасности);
- Осуществить реализацию взаимодействия ИС Банка и ЕСИА в соответствии с разделами 3, 3.1.2 и 3.4 методических рекомендаций по использованию Единой системы идентификации и аутентификации[19].
- Осуществить настройку доступа к сервису авторизации продуктивной ЕСИА в соответствии с разделом 8 приложения Б настоящего документа (см. Точка доступа к ЕСИА);
- Осуществить реализацию взаимодействия ИС Банка с ЕБС, посредством формирования, выгрузки и передачи вида сведений. Подробное описание представлено в приложение А настоящего документа (см. ПРИЛОЖЕНИЕ А. Вид сведений в единой системе межведомственного электронного взаимодействия «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию»);
- Осуществить реализацию автоматического фиксирования событий в вид сведений, для последующего направления в ЕБС в соответствии с разделом 4.1.4.1 настоящего документа;

[18] постоянная ссылка - https://smev3.gosuslugi.ru/portal/
[19] постоянная ссылка - https://digital.gov.ru/ru/documents/6186/

– Осуществить интеграцию ИС Банка с поставляемой библиотекой контроля качества в соответствии с руководствами пользователя БКК (по двум модальностям: голос и лицо)[20].

5.2 Регистрация Потребителя БДн

Для регистрации в качестве Потребителя БДн необходимо выполнить следующие обязательные условия:

1. Осуществить регистрацию в качестве Поставщика БДн (см. раздел 5.1).
2. Подключиться к ЕСИА в соответствии с актуальной версией Методических рекомендаций по использованию Единой системы идентификации и аутентификации[21].
3. Разработать web и мобильное приложения для интеграции с ЕБС в соответствии со сценарием, описанным в разделе 4.2 настоящего документа и с требованиями и рекомендациями, описанными в настоящем документе.
4. Зарегистрировать ИС в ЕБС в соответствии с Правилами и процедурами взаимодействия Участников биометрического взаимодействия.
5. Выполнить процедуры подключения ИС в соответствии с Правилами и процедурами взаимодействия Участников биометрического взаимодействия.

При подключении к ЕСИА необходимо пройти все процедуры в соответствии с регламентом, опубликованными на портале https://minsvyaz.ru/documents/.

При подключении к ЕБС необходимо пройти все процедуры в соответствии с Правилами и процедурами взаимодействия Участников биометрического взаимодействия.

Обязательное условие подключения Потребителя БДн, это успешное прохождение тестирования в интеграционной среде ЕБС. Успешное завершение тестирования должно быть подтверждено путём получения соответствующего уведомления от ЕБС.

5.2.1 Этапы настройки ИС Банка – Потребителя БДн

Для реализации взаимодействия ИС Банка с ЕБС необходимо осуществить следующие обязательные настройки:

[20] постоянная ссылка - https://bio.rt.ru/documents/software/
[21] постоянная ссылка - https://digital.gov.ru/ru/documents/6186/

- В случае отсутствия, осуществить реализацию взаимодействия ИС Банка и ЕСИА в соответствии с разделами 3, 3.1.2 и 3.4 методических рекомендаций по использованию Единой системы идентификации и аутентификации[22];
- В случае отсутствия, осуществить организацию защищенного канала связи до ЕСИА в соответствии с разделами 3, 3.1.2 и 3.4 методических рекомендаций по использованию Единой системы идентификации и аутентификации[23];
- В случае отсутствия, осуществить настройку доступа к сервису авторизации продуктивной ЕСИА в соответствии с разделом 8 приложения Б настоящего документа (см. Точка доступа к ЕСИА);
- В случае отсутствия, осуществить настройку получения маркера доступа и авторизационного кода в соответствии с разделом 4.2.1 настоящего документа приложением В.2 методических рекомендаций по использованию Единой системы идентификации и аутентификации[24] и разделом 4.2.1 настоящего документа;
- Осуществить реализацию взаимодействия ИС Банка с ЕБС и обмен информации посредством REST API в соответствии с приложением Б настоящего документа (см. ПРИЛОЖЕНИЕ Б. Описание интеграции внешних систем с Единой биометрической системой в процессе биометрической верификации);

Необходимо реализовать мобильное приложение Банка для взаимодействия с ЕБС:

- Реализовать поддержку операционных систем:
  - iOS не ниже версии 10;
  - Android не ниже версии 5.
- необходимо встроить ЕБС.SDK в мобильное приложение Банка в соответствии с описанием методов и классов в руководстве пользователя (см. ПРИЛОЖЕНИЕ Г. Руководство пользователя по работе с библиотекой ЕБС.Sdk).

[22] постоянная ссылка - https://digital.gov.ru/ru/documents/6186/
[23] постоянная ссылка - https://digital.gov.ru/ru/documents/6186/
[24] постоянная ссылка - https://digital.gov.ru/ru/documents/6186/

ПРИЛОЖЕНИЕ А. Вид сведений в единой системе межведомственного электронного взаимодействия «Универсальный вид сведений для приёма заявлений на биометрическую регистрацию»

1. Общие сведения

Описаны способы реализации Вида сведений по версии методических рекомендаций СМЭВ 3.4.0.0.

Формат ВС разработан с использованием языка описания схем данных XML Shema Definition (XSD) и соответствует следующим правилам:

- Для каждого вида сведений один из элементов, описанных на корневом уровне схемы, представляет собой «корневой элемент запроса».
- Для каждого вида сведений, кроме передаваемых с использованием широковещательных рассылок, один из элементов, описанных на корневом уровне схемы, представляет собой «корневой элемент ответа».
- Для каждого вида сведений корневой элемент запроса, и корневой элемент ответа описаны в одной схеме (имеет одно и то же пространство имён схемы). При этом схема может разбита на несколько XML-документов (конструкция xs:include), а также ссылаться на другие XML-схемы (конструкция xs:import).

Организация сеанса обмена ВС использует инициативный сеанс обмена. В данном случае сообщение-запрос содержит весь массив передаваемых сведений, которые информационная система – инициатор сеанса обмена намерена передать. А сообщение-ответ должен содержать сведения, описывающие факт получения сведений от инициатора.

Состав передаваемой информации и описание полей запроса приведены в таблице ниже.

Описание полей запроса

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип
1	RegisterBiometricDataRequestType	Запрос на регистрацию биометрических образцов с дополнительной информации	Обязательно для заполнения	complexType

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип
2	RegisterBiometricDataType	Класс описывающий биометрический образец и его метаинформацию	Обязательно для заполнения	complexType
3	BiometricDataType	Набор элементов биометрической информации с указанием модальности	Обязательно для заполнения	complexType

Описание полей ответа на запрос

№	Код поля	Описание поля	Требования к заполнению	Способ заполнения/Тип
1.	RegisterBiometricDataResponseType	Ответ с результатами регистрации биометрических образцов	Обязательно для заполнения	complexType
2.	RegistrarResultType	Перечень результатов регистрации образцов	Обязательно для заполнения	complexType

Описание комплексных типов полей

№	Код поля	Описание поля	Требования к заполнению	Способ заполнения/Тип
1.	**RegisterBiometricDataRequestType**	**Запрос на регистрацию биометрических образцов с дополнительной информацией**	**Обязательно для заполнения**	**complexType**
1.1	RegistrarMnemonic	Мнемоника информационной системы регистратора, полученая при	Обязательно для заполнения	type="tns:string-50"

№	Код поля	Описание поля	Требования к заполнению	Способ заполнения/Тип
		регистрации в СМЭВ		
1.2	BiometricData	Набор регистрируемых биометрических образцов	Обязательно для заполнения	tns:RegisterBiometricDataType maxOccurs="100"
1.3	EmployeeId	Идентификатор сотрудника, осуществляющего регистрацию	Обязательно для заполнения	type="tns:string-50"
2.	**RegisterBiometricDataType**	**Класс описывающий биометрический образец и его метаинформацию**	**Обязательно для заполнения**	**complexType**
2.1	Id	Уникальный идентификатор биометрического образца в рамках запроса	Обязательно для заполнения	type="xs:ID"
2.2	Date	Дата и время создания биометрического образка для регистрации, заполняется в зоне UTC.	Обязательно для заполнения	type="xs:dateTime"
2.3	RaId	Идентификатор центра обслуживания в реестре поставщика идентификации Idp В поле Raid указывается идентификатор ЦО в ЕСИА (если регистрация клиентов проводится через СМЭВ) или мнемоника ИС	Обязательно для заполнения	type="tns:string-36"

№	Код поля	Описание поля	Требования к заполнению	Способ заполнения/Тип
		Участника (если регистрация клиентов проводится через import)		
2.4	PersonId	Уникальный идентификатор субъекта регистрации в рамках его поставщика	Обязательно для заполнения	type="tns:string-100"
2.5	IdpMnemonic	Мнемоника поставшика идентификации субъекта регистрации	Обязательно для заполнения	type="tns:string-50"
2.6	Data	Набор элементов биометрической информации с указанием модальности	Обязательно для заполнения	tns:BiometricDataType maxOccurs="unbounded"
2.7	PersonMetadata	Метаданные субъекта регистрации	Обязательно для заполнения	tns:MetadataType maxOccurs="unbounded"
3	**BiometricDataType**	**Набор элементов биометрической информации с указанием модальности**	**Обязательно для заполнения**	**complexType**
3.1	Modality	Мнемоника модальности биометрического образца	Обязательно для заполнения	type="tns:string-20"
3.2	AttachmentRef*	Ссылка на вложение	Обязательно для заполнения	tns:AttachmentRefType
3.3	BioMetadata	Метаданные, прикрепляемые к биометрическому образцу	Необязательно для заполнения	tns:MetadataType minOccurs="0"

№	Код поля	Описание поля	Требования к заполнению	Способ заполнения/Тип
4	**RegisterBiometricDataResponseType**	**Ответ с результатами регистрации биометрических образцов**	**Обязательно для заполнения**	**complexType**
4.1	RegistrarResult	Перечень результатаов регистрации образцов	Обязательно для заполнения	type="tns:RegistrarResultType" maxOccurs="100"
5	**RegistrarResultType**	**Статус регистрации образца**	**Обязательно для заполнения**	**complexType**
5.1	Id	Идентификатор образца запроса	Обязательно для заполнения	type="tns:string-50"
5.2	Code	Код статуса	Обязательно для заполнения	type="tns:ResultCodeType"
5.3	Description	Описание в текстовом виде	Необязательно для заполнения	type="tns:string-500" minOccurs="0"
6	**ResultCodeType**	**Перечисление кодов статуса**	**Обязательно для заполнения**	**complexType**
7	**MetadataType**	**Комплексный тип для передачи метаданных**	**Обязательно для заполнения**	**complexType**
7.1	Key	Ключ значения метаданных	Обязательно для заполнения Недопускается повторение ключей значения метаданных PersonMetadata в рамках одного BiometricData	type="tns:string-50"
7.2	Value	Значение метаданных	Обязательно для заполнения	type="tns:string"
8	**AttachmentRefType**	**Данные о ссылке на вложение**	**Обязательно для заполнения**	**complexType**

№	Код поля	Описание поля	Требования к заполнению	Способ заполнения/Тип
8.1	AttachmentId	Ссылка на вложение	Обязательно для заполнения Не допускается повторение	type="tns:string" use="required"

* для передачи файлов биометрических образцов должно использоваться файловое хранилище СМЭВ. Атрибутом элемента **AttachmentRef** является **attachmentId**, который содержит идентификатор записи в файловом хранилище СМЭВ. Пересылка вложений должна осуществлять с использованием файлового хранилища (раздел 5 методических рекомендаций по работе с ЕСМЭВ 3.4.0.3). Принимаются вложения со следующими **MimeType**: image/png, image/jpeg, audio/pcm. Если значение поля MimeType отличается от указанных, то возвращается ошибка **NO_DATA**.

Описание видов метаданных поля BioMetadata

№	Код поля	Значение поля	Причина	Комментарий
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
		digits_desc	На записи произнесены цифры в убывающем порядке	

№	Код поля	Значение поля	Причина	Комментарий
		digits_random	На записи произнесены цифры в случайном порядке	модальности голос.
		text	На записи произнесен текст	

Где <part> - номер склеенной части звуковой записи, целые числа начиная с 1.

Описание видов метаданных поля PersonMetadata

Описание представлено в разделе 4.1.4.1.

Описание кодов статуса ResultCodeType

№	Значение поля	Описание	Внешнее описание
1	SUCCESS	Регистрация прошла успешно	Регистрация прошла успешно.
2	SUCCESS	Адаптация прошла успешно.	Адаптация прошла успешно.
3	NO_SUCH_MODALITY	Неподдерживаемая модальность	Ошибка: EBS-02020. Регистрация прошла не успешно. Модальности типа [%s] не поддерживается в системе
4	NO_BUILD_TEMPLATE	Не удалось построить БКШ по модальности	Ошибка: EBS-02021. Регистрация прошла не успешно. Не удалось создать биометрический шаблон по модальностям: [%s].
5	NO_DATA	Отсутствуют биометрические данные по модальностям	Ошибка: EBS-02022. Отсутствуют биометрические данные по модальностям: [%s].
6	ACCESS_DENIED	Данный провайдер идентификации не найден в системе	Ошибка: EBS-02030. Отказано в доступе. Указанный провайдер идентификации отсутствует в системе. Свяжитесь с администрацией ЕБС.
7	ACCESS_DENIED	Данный провайдер идентификации заблокирован в системе	Ошибка: EBS-02031. Отказано в доступе. Указанный провайдер идентификации заблокирован в системе. Свяжитесь с администрацией ЕБС.

№	Значение поля	Описание	Внешнее описание
8	ACCESS_DENIED	Данная ИС не найдена в системе	Ошибка: EBS-02040. Отказано в доступе. Указанная ИС отсутствует в системе. Свяжитесь с администрацией ЕБС.
9	ACCESS_DENIED	Данная ИС неактивена в системе	Ошибка: EBS-02041. Отказано в доступе. Указанная ИС заблокирована в системе. Свяжитесь с администрацией ЕБС.
10	NO_BUILD_TEMPLATE	Биометрические образцы не прошли проверку качества, с указанием ошибки БКК. Расшифровка кодов ошибок БКК находится на сайте (по ссылке - https://bio.rt.ru/documents/software/) в Руководстве пользователя БКК	Ошибка: EBS-02023. Биометрические образцы не прошли проверку качества. Результат проверки: <BKK_ERRORS>
11	ACCESS_DENIED	Тип информационной системы не соответствует требованиям	Ошибка: EBS-02042. Отказано в доступе. Указанная ИС не зарегистрирована в системе как поставщик БО. Свяжитесь с администрацией ЕБС.
12	NO_DATA	Недоступность ФХ СМЭВ	Ошибка: EBS-02025. Не удалось загрузить из ФХ СМЭВ данные по модальностям: [%s].
13	INTERNAL_ERROR	Недоступность ЕСИА, непредвиденные ошибки.	Ошибка: EBS-02010. В процессе обработки запроса произошла ошибка. Биометрический шаблон не создан.
14	INTERNAL_ERROR	Некорректная работа коннектора к СМЭВ	Ошибка: EBS-02011. В процессе обработки запроса произошла ошибка. Процесс регистрации не был запущен корректно.
15	NO_DATA	Проблемы с ФХ СМЭВ. Отсутствие обязательных данных для данной регистрации	Ошибка: EBS-02024. Отсутствуют обязательные данные: [%s].

Описание кодов возвратов при ошибках и неуспешных проверках

№	Код поля	Значение поля	Причина
1.	RequestRejected/ RejectionReasonCode	UNKNOWN_REQUEST_DESCRIPTION	ФЛК запроса не пройден.
2.	RequestRejected/ RejectionReasonCode	ACCESS_DENIED	Принято решение об отказе в предоставлении сведений действий в случае отсутствия прав на получение информации.
3.	RequestRejected/ RejectionReasonCode	NO_DATA	Не найдены данные по указанным в запросе параметрам.
4.	RequestRejected/ RejectionReasonCode	FAILURE	Ошибка при предоставлении сведений

Примечание: Обязательно должны в явном виде присутствовать коды мотивированного отказа в предоставлении сведений по причинам:

- Отсутствия запрашиваемой информации;
- Отказа в предоставлении доступа к запрашиваемой информации (в данном сервисе не осуществляется).

Подписание производится КСКП заявителя в соответствии с требованиями МР СМЭВ 3.xx.

Запрос вида сведений, передаваемый в составе СМЭВ 3-конверта (//MessagePrimaryContent) и в архиве должны быть полностью идентичны.

2. Описание вложений в составе пакета запроса вида сведений

Биометрические образцы должны передаваться посредством вложений ВС. Вложения передаются посредством Файлового Хранилища СМЭВ. Пересылка вложений с использованием файлового хранилища СМЭВ должно удовлетворять методических рекомендациям по работе с ЕСМЭВ.

ВС разработан с учётом возможности передачи на биометрическую регистрацию идентификатора регистрируемого пользователя как идентификатора учётной записи

пользователя, предоставляемого Провайдером идентификации (IdP) – участником биометрического взаимодействия.

Метод регистрации биометрических данных позволяет принимать как одиночные, так и пакетные запросы на регистрацию биометрических данных

3. Примеры XML-файлов

3.1. XSD-схема Вида сведений

Основная XSD-схема Вида сведений описана в таблице.

Основная схема: nbp-register-biometric.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:tns="urn://x-artefacts-nbp-rtlabs-ru/register/1.2.1"
        elementFormDefault="qualified"
        targetNamespace="urn://x-artefacts-nbp-rtlabs-ru/register/1.2.1"
        xmlns:vc="http://www.w3.org/2007/XMLSchema-versioning"
        vc:minVersion="1.1">
    <xs:annotation>
        <xs:documentation>Универсальный вид сведений для приёма заявлений на
биометрическую регистрацию</xs:documentation>
    </xs:annotation>

    <xs:element name="RegisterBiometricDataRequest"
type="tns:RegisterBiometricDataRequestType">
        <xs:unique name="attachmentId_must_be_unique">
            <xs:annotation>
                <xs:documentation>
                    Ограничение на то, что attachmentId должны быть уникальными в
рамках одного заявления на биометрическую регистрацию
                </xs:documentation>
            </xs:annotation>
            <xs:selector xpath=".//tns:AttachmentRef"/>
            <xs:field xpath="@attachmentId"/>
        </xs:unique>
        <xs:unique name="personId_must_be_unique">
            <xs:annotation>
                <xs:documentation>
                    Ограничение на то, что PersonId должны быть уникальными в
рамках одного заявления на биометрическую регистрацию
                </xs:documentation>
            </xs:annotation>
            <xs:selector xpath=".//tns:PersonId"/>
            <xs:field xpath="."/>
        </xs:unique>
    </xs:element>

    <xs:element name="RegisterBiometricDataResponse"
type="tns:RegisterBiometricDataResponseType"/>

    <xs:complexType name="RegisterBiometricDataRequestType">
        <xs:annotation>
            <xs:documentation>Запрос на регистрацию биометрических образцов с
дополнительной информацией</xs:documentation>
        </xs:annotation>
```

```
        <xs:sequence>
            <xs:element name="RegistrarMnemonic" type="tns:string-50">
                <xs:annotation>
                    <xs:documentation>Мнемоника информационной системы поставщика
БДн</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="EmployeeId" type="tns:string-50">
                <xs:annotation>
                    <xs:documentation>Идентификатор сотрудника осуществляющего
регистрацию (Справочник идентификаторов ведется банком)</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="BiometricData" type="tns:RegisterBiometricDataType"
maxOccurs="100">
                <xs:annotation>
                    <xs:documentation>Набор регистрируемых биометрических
образцов</xs:documentation>
                </xs:annotation>
                <xs:unique name="person_metadata_key_must_be_unique">
                    <xs:annotation>
                        <xs:documentation>
                            Ограничение на то, что Key метаданных PersonMetadata
должны быть уникальными в рамках одного BiometricData
                        </xs:documentation>
                    </xs:annotation>
                    <xs:selector xpath=".//tns:PersonMetadata/tns:Key"/>
                    <xs:field xpath="."/>
                </xs:unique>
                <xs:unique name="modality_must_be_unique">
                    <xs:annotation>
                        <xs:documentation>
                            Ограничение на то, что Modality должны быть
уникальными в рамках одного Data
                        </xs:documentation>
                    </xs:annotation>
                    <xs:selector xpath=".//tns:Data/tns:Modality"/>
                    <xs:field xpath="."/>
                </xs:unique>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="RegisterBiometricDataType">
        <xs:annotation>
            <xs:documentation>Класс описывающий биометрический образец и его
метаинформацию</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="Id" type="xs:ID">
                <xs:annotation>
                    <xs:documentation>Уникальный идентификатор биометрического
образца в рамках запроса</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Date" type="xs:dateTime">
                <xs:annotation>
                    <xs:documentation>Дата и время создания биометрического
образка для регистрации</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="RaId" type="tns:string-36">
                <xs:annotation>
                    <xs:documentation> Идентификатор центра обслуживания в
реестре поставщика идентификации Idp </xs:documentation>
                </xs:annotation>
```

```
            </xs:element>
            <xs:element name="PersonId" type="tns:string-100">
                <xs:annotation>
                    <xs:documentation>Уникальный идентификатор субъекта
регистрации в рамках его поставщика</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="IdpMnemonic" type="tns:string-50">
                <xs:annotation>
                    <xs:documentation>Мнемоника поставшика идентификации субъекта
регистрации</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Data" type="tns:BiometricDataType" maxOccurs="30">
                <xs:annotation>
                    <xs:documentation>Набор элементов биометрической информации с
указанием модальности</xs:documentation>
                </xs:annotation>
                <xs:unique name="metadata_key_must_be_unique">
                    <xs:annotation>
                        <xs:documentation>
                            Ограничение на то, что Key метаданных BioMetadata
должны быть уникальными в рамках одного Data
                        </xs:documentation>
                    </xs:annotation>
                    <xs:selector xpath=".//tns:BioMetadata/tns:Key"/>
                    <xs:field xpath="."/>
                </xs:unique>
            </xs:element>
            <xs:element name="PersonMetadata" type="tns:MetadataType"
maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>Метаданные субъекта
регистрации</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="BiometricDataType">
        <xs:sequence>
            <xs:element name="Modality" type="tns:string-20">
                <xs:annotation>
                    <xs:documentation>Мнемоника модальности биометрического
образца</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="AttachmentRef" type="tns:AttachmentRefType">
                <xs:annotation>
                    <xs:documentation>Ссылка на вложение</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="BioMetadata" type="tns:MetadataType" minOccurs="0"
maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>Метаданные биометрического
образца</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="MetadataType">
        <xs:sequence>
            <xs:element name="Key" type="tns:string-50">
                <xs:annotation>
```

```
                    <xs:documentation>Ключевое значение
метаданных</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Value" type="tns:string">
                <xs:annotation>
                    <xs:documentation>Значение метаданных</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="RegisterBiometricDataResponseType">
        <xs:annotation>
            <xs:documentation>Ответ с результатами регистрации биометрических
образцов</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="RegistrarResult" type="tns:RegistrarResultType"
maxOccurs="100">
                <xs:annotation>
                    <xs:documentation>Перечень результатаов регистрации
образцов</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="RegistrarResultType">
        <xs:annotation>
            <xs:documentation>Статус регистрации образца</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="Id" type="tns:string-50">
                <xs:annotation>
                    <xs:documentation>Ссылка на идентификатор
образца</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Code" type="tns:ResultCodeType">
                <xs:annotation>
                    <xs:documentation>Код статуса</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Description" type="tns:string-500" minOccurs="0">
                <xs:annotation>
                    <xs:documentation>Описание в текстовом
виде</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="ResultCodeType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="SUCCESS"/>
            <xs:enumeration value="NO_SUCH_MODALITY"/>
            <xs:enumeration value="NO_BUILD_TEMPLATE"/>
            <xs:enumeration value="NO_DATA"/>
            <xs:enumeration value="NO_METADATA"/>
            <xs:enumeration value="ACCESS_DENIED"/>
            <xs:enumeration value="INTERNAL_ERROR"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="string">
        <xs:restriction base="xs:string">
```

```
            <xs:minLength value="1"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="string-50">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="50"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="string-20">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="20"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="string-500">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="500"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="string-100">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="100"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="string-36">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="36"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="AttachmentRefType">
        <xs:annotation>
            <xs:documentation>
                Ссылка из содержательной части запроса (заявки, ответа) на
вложение, находящееся в том же
                СМЭВ-сообщении.
            </xs:documentation>
        </xs:annotation>
        <xs:attribute name="attachmentId" type="tns:string" use="required">
            <xs:annotation>
                <xs:documentation>
                    Идентификатор вложения, на которое ссылаемся. Должен быть
равен значению
                    //{urn://x-artefacts-smev-gov-ru/smev-core/client-
interaction/basic/1.0}AttachedFile[n]/Id/text()
                    того вложения, на которое нужно сослаться.
                </xs:documentation>
            </xs:annotation>
        </xs:attribute>
    </xs:complexType>
</xs:schema>
```

3.2. Эталонные сообщения

Эталонные примеры запроса и ответа приведены в таблицах.

Контрольный пример запроса RegisterBiometricDataRequest.xml

```
<tns:RegisterBiometricDataRequest xmlns:tns="urn://x-artefacts-nbp-rtlabs-
ru/register/1.2.1">
    <tns:RegistrarMnemonic>RTK027</tns:RegistrarMnemonic>
    <tns:EmployeeId>123-456-789 00</tns:EmployeeId>
    <tns:BiometricData>
        <tns:Id>ID-1</tns:Id>
        <tns:Date>2017-07-31T16:54:52+03:00</tns:Date>
        <tns:RaId>0c2c345f-cd7b-4011-9f3b-65095ab4c186</tns:RaId>
        <tns:PersonId>1000317495</tns:PersonId>
        <tns:IdpMnemonic>ESIA</tns:IdpMnemonic>
        <tns:Data>
            <tns:Modality>SOUND</tns:Modality>
            <tns:AttachmentRef attachmentId="ef37b493-e94f-4f27-9e86-
f4cd80f1057f"/>
            <tns:BioMetadata>
                <tns:Key>voice_1_start</tns:Key>
                <tns:Value>00.000</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_1_end</tns:Key>
                <tns:Value>10.074</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_1_desc</tns:Key>
                <tns:Value>digits_asc</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_2_start</tns:Key>
                <tns:Value>10.696</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_2_end</tns:Key>
                <tns:Value>20.673</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_2_desc</tns:Key>
                <tns:Value>digits_desc</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_3_start</tns:Key>
                <tns:Value>21.217</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_3_end</tns:Key>
                <tns:Value>30.980</tns:Value>
            </tns:BioMetadata>
            <tns:BioMetadata>
                <tns:Key>voice_3_desc</tns:Key>
                <tns:Value>digits_random</tns:Value>
            </tns:BioMetadata>
        </tns:Data>
        <tns:Data>
            <tns:Modality>PHOTO</tns:Modality>
            <tns:AttachmentRef attachmentId="397af8d0-d456-4dc1-9353-
1d6822a02200"/>
        </tns:Data>
        <tns:PersonMetadata>
            <tns:Key>total_reg_time_start</tns:Key>
            <tns:Value>2019-06-11 14:30:27</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>total_reg_time_end</tns:Key>
            <tns:Value>2019-06-11 15:30:27</tns:Value>
```

```
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>new_client_time_start</tns:Key>
            <tns:Value>2019-06-11 14:31:09</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>new_client_time_end</tns:Key>
            <tns:Value>2019-06-11 14:32:51</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>consent_time_start</tns:Key>
            <tns:Value>2019-06-11 14:33:05</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>consent_time_end</tns:Key>
            <tns:Value>2019-06-11 14:34:15</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>photo_time_start_1</tns:Key>
            <tns:Value>2019-06-11 14:36:19</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>photo_time_end_1</tns:Key>
            <tns:Value>2019-06-11 14:37:43</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>front_bqc_estimators_photo_1</tns:Key>
            <tns:Value>{"code": 67108864, "version": { "library": "1.0.9.0",
"configuration": "v1", "service": "1.0.8.10b4" }, "metadata": { "length": {
"value": 1139.000, "state": "passed" }, "channels": { "value": 3.000, "state":
"passed" }, "depth": { "value": 8.000, "state": "passed" }, "head_rx": { "value":
-10.559, "state": "failed" }, "head_ry": { "value": 0.903, "state": "passed" },
"head_rz": { "value": -0.321, "state": "passed" }, "eyes_distance": { "value":
153.381, "state": "passed" } }}</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_direct_time_start_1</tns:Key>
            <tns:Value>2019-06-11 14:38:23</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_direct_time_end_1</tns:Key>
            <tns:Value>2019-06-11 14:39:05</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>front_bqc_estimators_sound_direct_1</tns:Key>
            <tns:Value>{"code": 67108864, "version": { "library": "1.0.9.0",
"configuration": "v1", "service": "1.0.8.10b4" }, "metadata": { "signalnoise": {
"value": 14, "state": "passed" }, "duration": { "value": 30, "state": "passed" },
"simplerate": { "value": 17000, "state": "passed" }, "channels": { "value": 1,
"state": "failed" }, "length": { "value": 1139.000, "state": "passed" }, "depth":
{ "value": 24, "state": "passed" }, "frequency": { "value": 3200.00, "state":
"passed" }, "telephonyborder": { "value": 7200, "state": "passed" }
}}</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_reverse_time_start_1</tns:Key>
            <tns:Value>2019-06-11 14:39:15</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_reverse_time_end_1</tns:Key>
            <tns:Value>2019-06-11 14:39:29</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>front_bqc_estimators_sound_reverse_1</tns:Key>
```

```
            <tns:Value>{"code": 67108864, "version": { "library": "1.0.9.0",
"configuration": "v1", "service": "1.0.8.10b4" }, "metadata": { "signalnoise": {
"value": 14, "state": "passed" }, "duration": { "value": 30, "state": "passed" },
"simplerate": { "value": 17000, "state": "passed" }, "channels": { "value": 1,
"state": "failed" }, "length": { "value": 1139.000, "state": "passed" }, "depth":
{ "value": 24, "state": "passed" }, "frequency": { "value": 3200.00, "state":
"passed" }, "telephonyborder": { "value": 7200, "state": "passed" }
}}</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_random_time_start_1</tns:Key>
            <tns:Value>2019-06-11 14:39:40</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_random_time_end_1</tns:Key>
            <tns:Value>2019-06-11 14:40:00</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>front_bqc_estimators_sound_random_1</tns:Key>
            <tns:Value>{"code": 67108864, "version": { "library": "1.0.9.0",
"configuration": "v1", "service": "1.0.8.10b4" }, "metadata": { "signalnoise": {
"value": 14, "state": "passed" }, "duration": { "value": 30, "state": "passed" },
"simplerate": { "value": 17000, "state": "passed" }, "channels": { "value": 1,
"state": "failed" }, "length": { "value": 1139.000, "state": "passed" }, "depth":
{ "value": 24, "state": "passed" }, "frequency": { "value": 3200.00, "state":
"passed" }, "telephonyborder": { "value": 7200, "state": "passed" }
}}</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>sound_all_time_end_1</tns:Key>
            <tns:Value>2019-06-11 14:40:25</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>front_bqc_estimators_sound_all_1</tns:Key>
            <tns:Value>{"code": 67108864, "version": { "library": "1.0.9.0",
"configuration": "v1", "service": "1.0.8.10b4" }, "metadata": { "signalnoise": {
"value": 14, "state": "passed" }, "duration": { "value": 30, "state": "passed" },
"simplerate": { "value": 17000, "state": "passed" }, "channels": { "value": 1,
"state": "failed" }, "length": { "value": 1139.000, "state": "passed" }, "depth":
{ "value": 24, "state": "passed" }, "frequency": { "value": 3200.00, "state":
"passed" }, "telephonyborder": { "value": 7200, "state": "passed" }
}}</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>bank_find_profile_time_start_1</tns:Key>
            <tns:Value>2019-06-11 14:41:02</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>bank_find_profile_time_end_1</tns:Key>
            <tns:Value>2019-06-11 14:41:20</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>esia_find_account_msg_id</tns:Key>
            <tns:Value>0s0ca258-40b4-11e9-b4ds-998984r325nf</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>esia_confirm_msg_id</tns:Key>
            <tns:Value>0q3ca644-40b4-11e9-s029-887873e214bd</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>esia_register_by_simplified_msg_id</tns:Key>
            <tns:Value>0f2ca369-40b4-11e9-b028-555221w421vs</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>esia_recover_msg_id</tns:Key>
```

```
            <tns:Value>0a8ca516-40b4-11e9-fd9d-159753d852gc</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>name_equipment_camera</tns:Key>
            <tns:Value>hp proVision</tns:Value>
        </tns:PersonMetadata>
        <tns:PersonMetadata>
            <tns:Key>name_equipment_microphone</tns:Key>
            <tns:Value>microphone ainane</tns:Value>
        </tns:PersonMetadata>
    </tns:BiometricData>
</tns:RegisterBiometricDataRequest>
```

Контрольный пример ответа RegisterBiometricDataResponse.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:RegisterBiometricDataResponse xmlns:tns="urn://x-artefacts-nbp-rtlabs-
ru/register/1.2.1">
   <tns:RegistrarResult>
      <tns:Id>ID-1</tns:Id>
      <tns:Code>SUCCESS</tns:Code>
      <tns:Description>Регистрация прошла успешно.</tns:Description>
   </tns:RegistrarResult>
</tns:RegisterBiometricDataResponse>
```

Описание контрольного примера:

Идентификатор контрольного примера (xpath)	Пространство имен, используемое в xpath
//tns:RegisterBiometricDataRequest	tns=urn://x-artefacts-nbp-rtlabs-ru/register/1.2.1

Контрольный сценарий TestScenario.xslt

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsl:stylesheet
        version="2.0"
        xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
        xmlns:tns="urn://x-artefacts-nbp-rtlabs-ru/register/1.2.1">
    <xsl:output method="xml" indent="yes" encoding="UTF-8"/>

    <xsl:template match="/tns:RegisterBiometricDataRequest">
        <RegisterBiometricDataResponse xmlns="urn://x-artefacts-nbp-rtlabs-
ru/register/1.2.1">
            <xsl:for-each select="tns:BiometricData">
                <RegistrarResult>
                    <Id><xsl:value-of select="tns:Id"/></Id>
                    <xsl:choose>
                        <xsl:when test="tns:Data/tns:Modality = 'SOUND' or
tns:Data/tns:Modality = 'PHOTO'">
                            <Code>SUCCESS</Code>
                            <Description>Регистрация прошла
успешно.</Description>
                        </xsl:when>
                        <xsl:otherwise>
                            <Code>NO_DATA</Code>
                            <Description>Ошибка: EBS-02024. Отсутствуют
обязательные данные:
                            ['Отсутствует БО модальности photo', 'Отсутствует БО
модальности
                            sound'].</Description>
```

```
                        </xsl:otherwise>
                    </xsl:choose>
                </RegistrarResult>
            </xsl:for-each>
        </RegisterBiometricDataResponse>
    </xsl:template>
</xsl:stylesheet>
```

Описание контрольного примера:

Контрольный пример	Идентификатор контрольного примера (xpath)	Пространство имен, используемое в xpath	XSL файл для сценария
КП	//tns:RegisterBiometricDataRequest/tns:RegistrarMnemonic/text()='TEST01'	tns=urn://x-artefacts-nbp-rtlabs-ru/register/1.2.1	*TestScenario.xsl*

ПРИЛОЖЕНИЕ Б. Описание интеграции внешних систем с Единой биометрической системой в процессе биометрической верификации

1. Общее описание API Биометрической верификации

Процесс взаимодействия ИС Потребителя БДн реализовано посредством REST API. Архитектура REST (Representational State Transfer) подразумевает наличие клиент-серверной архитектуры. Клиент инициирует запросы к серверу, сервер обрабатывает их и возвращает ответ.

REST API определяет набор методов, к которым ИС Потребителя БДн может совершать запросы и получать ответы. Взаимодействие происходит по протоколу HTTP(S).

Список используемых в Системе методов REST API, а также необходимые параметры и возвращаемые значения, приведены ниже в данном документе.

2. Точка доступа к API Биометрической верификации

Базовый URL доступа к API Биометрической верификации (далее API верификации) в среде интеграционного тестирования:

https://ebs-int.rtlabs.ru/api

Базовые URL доступа к API Биометрической верификации (далее API верификации) в продуктивной среде:

http://10.112.132.254/api

http://10.112.132.253/api

При вызове адресов ЕБС в продуктивной среде необходимо использовать защищённую сеть передачи данных ПАО «Ростелеком». ИС Потребителя БДн может использовать любой/оба из указанных выше адресов в продуктивной среде.

Актуальные версии API верификации: «v1», «v2».

Формат версии: префикс «v» и целое число.

3. Поддерживаемые методы HTTP

Система поддерживает следующие методы HTTP:

– GET

– POST

Сервер должен поддерживать следующие типы контента запроса (HTTP-заголовок «Content-Type»):

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

Входные параметры метода передаются в виде строки запроса[25] (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[26], 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[27].

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 каждый входной параметр метода 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);
– заголовочное поле «Content-Type», принимающая значение в зависимости от контента, передаваемого в части:
    – выходные параметры метода: «application/json»;
    – биометрический образец: «application/octet-stream».

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

[25] Согласно RFC 3984, раздел 3.4
[26] Согласно RFC 3986, раздел 2.1
[27] Согласно RFC 7159

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.

4. Используемые коды ответов HTTP

Используемые Системой коды ответов HTTP приведены в таблицах ниже.

Коды ответа для API «v1»:

Коды ответа	Описание
200 OK	Вызов метода завершился успешно. Ответ Системы 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.)
403 Forbidden	Вызов метода завершился с ошибкой: аутентификация прошла успешно, но у пользователя нет доступа к ресурсу
500 Internal Server Error	Вызов метода завершился с ошибкой на стороне сервера (ЕБС). Код ошибки включен в HTTP BODY.

Все успешные ответы, не требующие перенаправления пользователя:

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

Все успешные ответы, требующие перенаправления пользователя:

- содержат код ответа HTTP 302;
- в заголовке Location указан URL, на который необходимо перенаправить пользователя.

Все ответы с ошибкой:

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

Коды ответа для API «v2»:

Коды ответа	Описание
200 OK	Вызов метода завершился успешно. Ответ Системы включен в HTTP BODY или в заголовок «Location», в этом случае 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.)
403 Forbidden	Вызов метода завершился с ошибкой: аутентификация прошла успешно, но у пользователя нет доступа к ресурсу
500 Internal Server Error	Вызов метода завершился с ошибкой на стороне сервера (ЕБС). Код ошибки включен в HTTP BODY.

Все успешные ответы, не требующие перенаправления пользователя:

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

Все успешные ответы, требующие перенаправления пользователя:

- содержат код ответа HTTP 200;
- в заголовке Location указан URL, на который необходимо перенаправить пользователя.

Все ответы с ошибкой:

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

Пример ответа с ошибкой:

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

{
  "code": "EBS-010101",
  "message": "Ошибка проверки маркера доступа"
}
```

Перечень общих для всех методов кодов «code» и описаний «message» ошибок приведен в таблице ниже. Ошибки, специфичные для конкретного метода приведены в соответствующем разделе описания метода.

Коды ошибок:

Код ответа HTTP	Значение параметра «code»	Описание (параметр «message»)
500	EBS-010001	Внутренняя ошибка API
500	EBS-010002	Сервис в настоящее время не может выполнить запрос из-за большой нагрузки или технических работ на сервере
400	EBS-010003	Неверный запрос
400	EBS-010004	Запрос не содержит обязательного параметра {название параметра}

5. Методы API Верификации «v1»

5.1. Метод «Старт верификации в ЕБС»

Метод запуска процесса биометрической верификации Пользователя в ЕБС. ИС Потребителя БДн в HTTP-заголовке «Authorization» должна:

- указать схему аутентификации[28] «Bearer»;
- передать специальный маркер доступа, полученный от ЕСИА в процессе авторизации пользователя.

Данный маркер доступа подписан ЭП ЕСИА и содержит в том числе следующие атрибуты:

- Идентификатор пользователя в ЕСИА;
- Мнемонику ИС Потребителя БДн в ЕСИА.

Тип контента HTTP-запроса: «application/json»

5.1.1. Вызов метода

POST /api/v1/verifications?redirect=*{redirect_uri}*

Где:

- *{v1}* – актуальная версия API;
- *{redirect}* - Значение параметра redirect, приведенное ниже.

[28] Согласно RFC 2617, раздел 1.2 и RFC 6750.

Входные параметры:

Наименование параметра	Значение	Описание
redirect	String	Обязательный параметр. Полный URL ИС Потребителя БДн, на который ЕБС осуществит перенаправление пользователя после удачной верификации.
metadata[29]	JSON Object	Обязательный параметр. Содержит перечень дополнительных данных об устройстве Пользователя.

Пример запроса:

```
POST /api/v1/verifications?redirect=https%3A%2F%2Ftest.bank.local%2Freturn_uri
HTTP/1.1
Host: ebs-int.rtlabs.ru
Content-Type: application/json
Authorization: Bearer {Специальный маркер доступа, полученный от ЕСИА}
Cache-Control: no-cache

{
        "metadata":{
                "date":"153016814952",
                "user_id":"898858745",
                "info_system":"888999555",
                "idp":"ESIA"
        }
}
```

5.1.2. Успешный ответ метода

В случае успешного ответа, метод возвращает сообщение HTTP Redirect (код состояния 302). В HTTP заголовке «Location» URL WEB-формы ЕБС, на который необходимо осуществить перенаправление пользователя для снятия биометрических образцов.

В составе данного URL передаются параметры, приведенные в таблице ниже.

Выходные параметры:

[29] описание параметров metadata приведено в разделе 7 «Спецификация параметров metadata» Приложения Б

Наименование параметра	Значение	Описание
session_id	String	Обязательный параметр. Идентификатор сессии верификации в Системе. Должен передаваться при последующих запросах методов.
redirect	String	Обязательный параметр. Полный URL ИС Потребителя БДн, переданный в параметрах запроса

Пример ответа:

```
HTTP/1.1 302 Found
  Location: https://ebs-
int.rtlabs.ru/ui/verification?session_id=SE9CF4FCEB7EE4160BCAF243D031607E3&redire
ct= https%3A%2F%2Ftest.bank.local%2Freturn_uri
```

5.1.3. Ошибки метода

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

Коды ошибок:

Код ответа HTTP	Значение параметра «code»	Описание (параметр «message»)
400	EBS-010201	Параметр redirect не установлен
400	EBS-010202	Незарегистрированный адрес для перенаправления (redirect)
400	EBS-010301	Пользователь не найден
400	EBS-010103	Маркер доступа не содержит обязательного параметра
401	EBS-010101	Ошибка проверки маркера доступа
401	EBS-010102	Ошибка проверки ЭП ЕСИА
401	EBS-010104	Маркер доступа просрочен
403	EBS-010109	Провайдеру идентификации запрещен доступ к ЕБС
403	EBS-010203	Системе-клиенту запрещен доступ к ЕБС
403	EBS-010110	Пользователю запрещен доступ к ЕБС

5.2. Методы обеспечения процедуры биометрической верификации в ЕБС

Методы обеспечения процесса биометрической верификации:

- Согласование методов сбора БО и Liveness;
- Приём БО на верификацию.

Данные методы являются внутренними и вызываются компонентами ЕБС по сбору БО (WEB-форма ЕБС / МП ЕБС).

5.2.1. Успешный результат процедуры биометрической верификации

В случае успешного прохождения биометрической верификации, Система возвращает сообщение HTTP Redirect (код состояния 302). В HTTP заголовке «Location» содержится URL ИС Потребителя БДн, для перенаправления пользователя после удачной верификации. ЕБС использует значение URL ИС Потребителя БДн, переданное в параметре «redirect» при вызове метода «Старт верификации в ЕБС».

В составе данного URL передаются параметры, приведенные в таблице ниже.

Наименование параметра	Значение	Описание
verify_token	String	Обязательный параметр. Контрольное значение (уникальный идентификатор, созданный ЕБС для ЕСИА), необходимое для завершения процедуры аутентификации в ЕСИА после получения результата верификации.
expired	Number	Обязательный параметр Время прекращения действия результата биометрической верификации пользователя в ЕСИА, в миллисекундах с 1 января 1970 г. 00:00:00 GMT. После указанного в параметре момента времени получение специального маркера доступа со скоупом ext_auth_result в ЕСИА будет невозможно.

Пример успешного ответа:

```
HTTP/1.1 302 Found
  Location:
https://test.bank.local/return_uri?verify_token=0BCAF243SE9CF4F607E3CEB7EE416D031
& expired=1499443407648
```

5.2.2. Ошибки

Если запрос метода поступил с WEB-формы ЕБС, в случае получения ошибки, WEB-форма предлагает пользователю вернуться в Банк: кнопка «Назад в банк», по нажатию на которую, WEB-форма перенаправляет пользователя на ИС Потребителя БДн по ссылке, содержащейся в параметре «redirect».

Если запрос метода поступил с МП ЕБС, в случае получения ошибки, МП ЕБС возвращает в МП Потребителя БДн код «resultCode» и объект с пустыми полями verifyToken и expired (см. ПРИЛОЖЕНИЕ Г. Руководство пользователя по работе с библиотекой ЕБС.Sdk).

5.3.Метод «Получение результата верификации»

Метод получения ИС Потребителя БДн расширенного результата биометрической верификации, содержащего в себе результат вычитания из единицы вероятности ложного совпадения по разным модальностям и общей вероятности ложного совпадения.

В HTTP-заголовке «Authorization» необходимо:

- указать схему аутентификации «Bearer»;
- передать специальный маркер доступа (access_token с разрешением на scope «openid» и «ext_auth_result»), полученный от ЕСИА.

Тип контента HTTP-запроса: «application/json»

5.3.1. Вызов метода

GET /api/v1/verifications/{session_id}/result

Где:

{v1} – актуальная версия API"*;*
{session_id} – идентификатор сессии верификации в Системе, полученный в ответе метода "Старт верификации в ЕБС".

Входные параметры:

Отсутствуют

Пример запроса:

```
GET /api/v1/verifications/D530D7AF1EFA47489653FC4CEA5AC625/result HTTP/1.1
```

```
Host: ebs-int.rtlabs.ru
Authorization: Bearer {Специальный маркер доступа, полученный от ЕСИА с
разрешением на scope "ext_auth_result"}
Cache-Control: no-cache
```

5.3.2. Успешный ответ метода

В случае успешного ответа, метод возвращает сообщение, содержащее следующие параметры:

Наименование параметра	Значение	Описание
extended_result	String	Обязательный параметр. Расширенный результат верификации, содержащий степени схожести (общая и по каждой из модальностей). Параметр передается в формате JWT токена[30].

Данный JWT токен состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATURE.

Каждая из частей токена представляет из себя Base64url Encoding значение.

1. HEADER – описание свойств токена, в тои числе описание используемого алгоритма для подписи.

   Пример:

   {"kid":"2277cf04-8bdd-47a6-8cb8-e7ac373e0bf8","alg":"GOST3410","typ":"JWT"}

   Где:

   “alg” – алгоритм шифрования (на текущий момент ЕБС поддерживает алгоритмы формирования электронной подписи ГОСТ Р 34.10-2012 и алгоритм криптографического хэширования ГОСТ Р 34.11-2012[31]);

   “typ” – тип токена (в ЕБС всегда имеет значение “JWT” (JSON Web Token));

   “kid” – идентификатор ключа.
2. PAYLOAD – непосредственно данные о токене и идентифицированном субъекте (или субъекте доступа).

[30] Согласно RFC 7519

[31] В интеграционной среде можно использовать также алгоритм формирования электронной подписи RS256 и алгоритм криптографического хэширования RSA SHA-256

Пример:

{"iss":"http:ebs-int.rtlabs.ru",
"sub":11111111,
"aud":"TEST_SYSTEM",
"nbf":1551940552,
"iat":1551940551,
"exp":1551941153,
"result":true,
"match":"{\"overall\":1.0,\"face\":0.999999899,\"voice\":1.0}"

Где:

iss - идентификатор организации, выпустившей токен;

nbf – время, ранее которого нельзя использовать токен (Unix time stamp в секундах);

iat – время создания токена (Unix time stamp в секундах);

exp – время окончания срока действия токена (Unix time stamp в секундах);

sub - идентификатор пользователя ЕСИА;

aud - мнемоника ИС Потребителя БДн в ЕСИА;

result - результат биометрической верификации;

match - содержит значения, вычисляемые как:

- *overall*: разность единицы и произведения вероятностей ложного совпадения по каждой из модальностей (1-ВЛС.лицо*ВЛС.голос);
- *face*: разность единицы и вероятности ложного совпадения по модальности «Лицо» (1-ВЛС.лицо);
- *voice*: разность единицы и вероятности ложного совпадения по модальности «Голос» (1-ВЛС.голос)

3. SIGNATURE – подпись в формате CAdES-T (содержащая доверенную метку времени) detached signature в кодировке UTF-8 от значений первых двух частей маркера доступа (HEADER.PAYLOAD).

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
{
"extended_result": "{Base64 JWT Token с расширенным результатом верификации}"
```

```
}
```

5.3.3. Ошибки метода

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

Код ответа HTTP	Значение параметра «code»	Описание
400	EBS-010302	Идентификатор сессии не найден
400	EBS-010303	Время жизни сессии истекло

6. Методы API Верификации «v2»

6.1. Метод «Старт верификации в ЕБС»

Метод запуска процесса биометрической верификации Пользователя в ЕБС. ИС Потребителя БДн в HTTP-заголовке «Authorization» должна:

- указать схему аутентификации[32] «Bearer»;
- передать специальный маркер доступа, полученный от ЕСИА в процессе авторизации пользователя.

Данный маркер доступа подписан ЭП ЕСИА и содержит в том числе следующие атрибуты:

- Идентификатор пользователя в ЕСИА;
- Мнемонику ИС Потребителя БДн в ЕСИА.

Тип контента HTTP-запроса: «application/json»

6.1.1. Вызов метода

POST /api/v2/verifications?redirect=*{redirect_uri}*

Где:

- *{v2}* –версия API;
- *{redirect}* - Значение параметра redirect, приведенное ниже.

[32] Согласно RFC 2617, раздел 1.2 и RFC 6750.

Входные параметры:

Наименование параметра	Значение	Описание
redirect	String	Обязательный параметр. Полный URL ИС Потребителя БДн, на который ЕБС осуществит перенаправление пользователя после удачной верификации.
metadata[33]	JSON Object	Обязательный параметр. Содержит перечень дополнительных данных об устройстве Пользователя.

Пример запроса:

```
POST /api/v2/verifications?redirect=https%3A%2F%2Ftest.bank.local%2Freturn_uri
HTTP/1.1
Host: ebs-int.rtlabs.ru
Content-Type: application/json
Authorization: Bearer {Специальный маркер доступа, полученный от ЕСИА}
Cache-Control: no-cache

{
        "metadata":{
                "date":"153016814952",
                "user_id":"898858745",
                "info_system":"888999555",
                "idp":"ESIA"
        }
}
```

6.1.2. Успешный ответ метода

В случае успешного ответа, метод возвращает сообщение HTTP OK (код состояния 200). В HTTP заголовке «Location» URL WEB-формы ЕБС, на который необходимо осуществить перенаправление пользователя для снятия биометрических образцов.

В составе данного URL передаются параметры, приведенные в таблице ниже.

Выходные параметры:

[33] описание параметров metadata приведено в разделе 7 «Спецификация параметров metadata» Приложения Б

Наименование параметра	Значение	Описание
session_id	String	Обязательный параметр. Идентификатор сессии верификации в Системе. Должен передаваться при последующих запросах методов.
redirect	String	Обязательный параметр. Полный URL ИС Потребителя БДн, переданный в параметрах запроса

Пример ответа:

```
HTTP/1.1 200 OK
  Location: https://ebs-
int.rtlabs.ru/ui/verification?session_id=SE9CF4FCEB7EE4160BCAF243D031607E3&redire
ct= https%3A%2F%2Ftest.bank.local%2Freturn_uri
```

6.1.3. Ошибки метода

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

Коды ошибок:

Код ответа HTTP	Значение параметра «code»	Описание (параметр «message»)
400	EBS-010201	Параметр redirect не установлен
400	EBS-010202	Незарегистрированный адрес для перенаправления (redirect)
400	EBS-010301	Пользователь не найден
400	EBS-010103	Маркер доступа не содержит обязательного параметра
401	EBS-010101	Ошибка проверки маркера доступа
401	EBS-010102	Ошибка проверки ЭП ЕСИА
401	EBS-010104	Маркер доступа просрочен
403	EBS-010109	Провайдеру идентификации запрещен доступ к ЕБС
403	EBS-010203	Системе-клиенту запрещен доступ к ЕБС
403	EBS-010110	Пользователю запрещен доступ к ЕБС

6.2. Методы обеспечения процедуры биометрической верификации в ЕБС

Методы обеспечения процесса биометрической верификации:

- Согласование методов сбора БО и Liveness;
- Приём БО на верификацию.

Данные методы являются внутренними и вызываются компонентами ЕБС по сбору БО (WEB-форма ЕБС / МП ЕБС).

6.2.1. Успешный результат процедуры биометрической верификации

В случае успешного прохождения биометрической верификации, Система возвращает сообщение HTTP OK (код состояния 200). В HTTP заголовке «Location» содержится URL ИС Потребителя БДн, для перенаправления пользователя после удачной верификации. ЕБС использует значение URL ИС Потребителя БДн, переданное в параметре «redirect» при вызове метода «Старт верификации в ЕБС».

В составе данного URL передаются параметры, приведенные в таблице ниже.

Наименование параметра	Значение	Описание
verify_token	String	Обязательный параметр. Контрольное значение (уникальный идентификатор, созданный ЕБС для ЕСИА), необходимое для завершения процедуры аутентификации в ЕСИА после получения результата верификации.
expired	Number	Обязательный параметр Время прекращения действия результата биометрической верификации пользователя в ЕСИА, в миллисекундах с 1 января 1970 г. 00:00:00 GMT. После указанного в параметре момента времени получение специального маркера доступа со скоупом ext_auth_result в ЕСИА будет невозможно.

Пример успешного ответа:

```
HTTP/1.1 200 OK
  Location:
https://test.bank.local/return_uri?verify_token=0BCAF243SE9CF4F607E3CEB7EE416D031
& expired=1499443407648
```

6.2.2. Ошибки

Если запрос метода поступил с WEB-формы ЕБС, в случае получения ошибки, WEB-форма предлагает пользователю вернуться в Банк: кнопка «Назад в банк», по нажатию на которую, WEB-форма перенаправляет пользователя на ИС Потребителя БДн по ссылке, содержащейся в параметре «redirect».

Если запрос метода поступил с МП ЕБС, в случае получения ошибки, МП ЕБС возвращает в МП Потребителя БДн код «resultCode» и объект с пустыми полями verifyToken и expired (см. ПРИЛОЖЕНИЕ Г. Руководство пользователя по работе с библиотекой ЕБС.Sdk).

6.3.Метод «Получение результата верификации»

Метод получения ИС Потребителя БДн расширенного результата биометрической верификации, содержащего в себе результат вычитания из единицы вероятности ложного совпадения по разным модальностям и общую вероятность ложного совпадения.

В HTTP-заголовке «Authorization» необходимо:

- указать схему аутентификации «Bearer»;
- передать специальный маркер доступа (access_token с разрешением на scope «openid» и «ext_auth_result»), полученный от ЕСИА.

Тип контента HTTP-запроса: «application/json»

6.3.1. Вызов метода

GET /api/v2/verifications/*{session_id}*/result

Где:

{v2} –версия API*;*
{session_id} – идентификатор сессии верификации в Системе, полученный в ответе метода "Старт верификации в ЕБС".

Входные параметры:

Отсутствуют

Пример запроса:

```
GET /api/v2/verifications/D530D7AF1EFA47489653FC4CEA5AC625/result HTTP/1.1
```

```
Host: ebs-int.rtlabs.ru
Authorization: Bearer {Специальный маркер доступа, полученный от ЕСИА с
разрешением на scope "ext_auth_result"}
Cache-Control: no-cache
```

6.3.2. Успешный ответ метода

В случае успешного ответа, метод возвращает сообщение, содержащее следующие параметры:

Наименование параметра	Значение	Описание
extended_result	String	Обязательный параметр. Расширенный результат верификации, содержащий степени схожести (общая и по каждой из модальностей). Параметр передается в формате JWT токена[34].

Данный JWT токен состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATURE.

Каждая из частей токена представляет из себя Base64url Encoding значение.

1. HEADER – описание свойств токена, в тои числе описание используемого алгоритма для подписи.

   Пример:

   {"kid":"2277cf04-8bdd-47a6-8cb8-e7ac373e0bf8","alg":"GOST3410","typ":"JWT"}

   Где:

   “alg” – алгоритм шифрования (на текущий момент ЕБС поддерживает алгоритмы формирования электронной подписи ГОСТ Р 34.10-2012 и алгоритм криптографического хэширования ГОСТ Р 34.11-2012[35]);

   “typ” – тип токена (в ЕБС всегда имеет значение “JWT” (JSON Web Token));

   “kid” – идентификатор ключа.
2. PAYLOAD – непосредственно данные о токене и идентифицированном субъекте (или субъекте доступа).

[34] Согласно RFC 7519

[35] В интеграционной среде можно использовать также алгоритм формирования электронной подписи RS256 и алгоритм криптографического хэширования RSA SHA-256

Пример:

{"iss":"http:ebs-int.rtlabs.ru",

"sub":11111111,

"aud":"TEST_SYSTEM",

"nbf":1551940552,

"iat":1551940551,

"exp":1551941153,

"result":true,

"match":"{\"overall\":1.0,\"face\":0.999999899,\"voice\":1.0}"

Где:

iss - идентификатор организации, выпустившей токен;

nbf – время, ранее которого нельзя использовать токен (Unix time stamp в секундах);

iat – время создания токена (Unix time stamp в секундах);

exp – время окончания срока действия токена (Unix time stamp в секундах);

sub - идентификатор пользователя ЕСИА;

aud - мнемоника ИС Потребителя БДн в ЕСИА;

result - результат биометрической верификации;

match - содержит значения, вычисляемые как:

- *overall*: разность единицы и произведения вероятностей ложного совпадения по каждой из модальностей (1-ВЛС.лицо*ВЛС.голос);
- *face*: разность единицы и вероятности ложного совпадения по модальности «Лицо» (1-ВЛС.лицо);
- *voice*: разность единицы и вероятности ложного совпадения по модальности «Голос» (1-ВЛС.голос)

3. SIGNATURE – подпись в формате CAdES-T (содержащая доверенную метку времени) detached signature в кодировке UTF-8 от значений первых двух частей маркера доступа (HEADER.PAYLOAD).

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
{
"extended_result": "{Base64 JWT Token с расширенным результатом верификации}"
}
```

6.3.3. Ошибки метода

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

Код ответа HTTP	Значение параметра «code»	Описание
400	EBS-010302	Идентификатор сессии не найден
400	EBS-010303	Время жизни сессии истекло

7. Спецификация параметров metadata

Все параметры metadata, перечисленные в таблице ниже, имеют тип String и обязательны к заполнению.

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.

Формат параметра metadata: **date,** должен соответствовать формату даты в составе специального маркера доступа, полученного от ЕСИА в процессе авторизации пользователя и переданного в Систему в составе запроса метода «Старт верификации в ЕБС».

Дополнительные данные об устройстве пользователя (metadata):

Наименование параметра	Описание	Формат	Пример
date	Дата и время начала операции (формирования запроса клиентом)	timestamp	1520467814933

Наименование параметра	Описание	Формат	Пример
time_zone	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
geolocation	Координаты (Геолокация): широта и долгота	latitude;longitude	51.7556415;55.1028652
local_ip_address	IP адрес устройства	ipv4/ipv6	127.0.0.0
rooted	Наличие jailbreak или root-доступа в операционной системе	true/false	true
operating_system	Операционная система устройства: − название; − версия	name version	Android 6.0.1
isp	Провайдер	name	MegaFon
advertising_id	Идентификатор рекламы устройства (AdID в Android и IDFA в iOS)	value	38400000-8cf0-11bd-b23e-10b96e40000d
screen	Разрешение экрана	width;height	1200;1920
dpi	Плотность экрана устройства - значение, единицы измерения плотности пикселей	value	320 Dpi

Наименование параметра	Описание	Формат	Пример
camera_id	Идентификатор камеры	name	2
locale	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
device_serial	Серийный номер мобильного устройства.	deviceNumber	0819da27
imei	IMEI - международный идентификатор мобильного оборудования	value	357719051789508
device_id	Уникальный идентификатор Android-устройства	value	d1b23ев2f3b480cb
device_manufacturer	Производитель устройства	name	asus
device_model	Модель устройства	name	Nexus 7
device_cpu	Информация о процессоре устройства	value	ARMv7 Processor rev 0 (v7l)
sim	Информация о SIM-карте: − оператор; − название оператора; − страна; − номер сим карты. Можно отдавать раздельно.	simOperator;simOperatorName;simCountryIso;simSerialNumber	25002;MegaFon;ru;897210285241754519

8. Точка доступа к ЕСИА

Для взаимодействия с продуктивной средой ЕСИА, необходимо использовать следующие каналы взаимодействия и адреса.

Доступ к Authorization endpoint ЕСИА должен осуществляться с клиентского устройства через сеть Интернет:

https://esia.gosuslugi.ru/aas/oauth2/ac

Доступ к Token endpoint ЕСИА должен осуществляться через защищённую сеть передачи данных ПАО «Ростелеком»:

https://172.16.104.200/aas/oauth2/te

Доступ к сервисам получения персональных данных клиента ЕСИА должен осуществляться через защищённую сеть передачи данных ПАО «Ростелеком»:

https://172.16.104.200/

ПРИЛОЖЕНИЕ В. Описание установки и настройки мобильного приложения на ОС Android

Процесс установки и настройки приложения приводится на рисунке ниже (см. Рисунок 10)

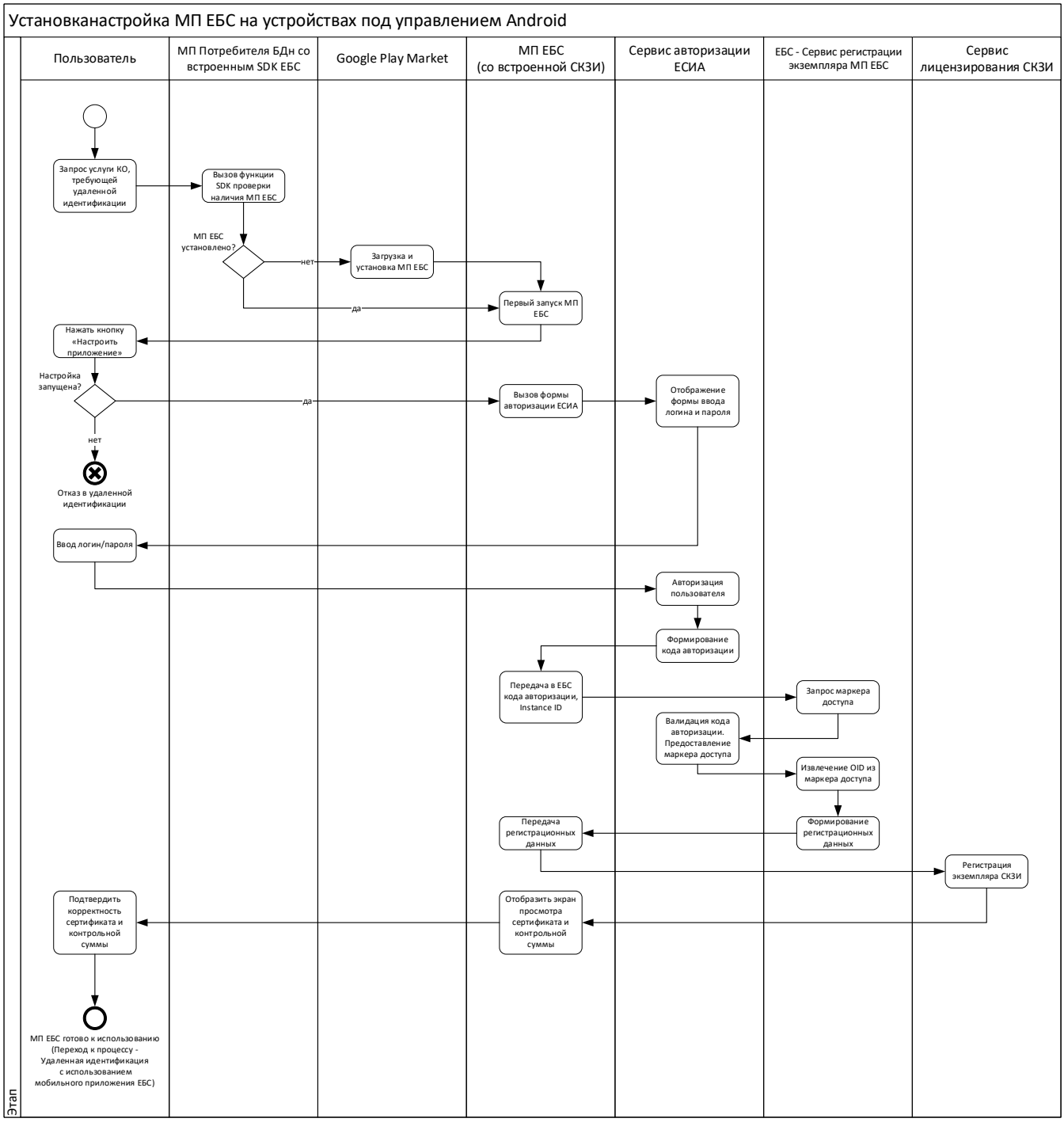

Рисунок 10 – Установка и настройка МП ЕБС на устройствах с ОС Android

Сценарий установки и настройки МП ЕБС на устройствах с ОС Android приведён в таблице ниже.

Мобильное приложение:
МП ЕБС

Цель:

- Установить и настроить МП ЕБС.

Роли:

- Пользователь;
- Google Play Market;
- МП Потребителя БДн;
- МП ЕБС;
- Сервис авторизации ЕСИА;
- Сервис регистрации экземпляра МП ЕБС;
- Сервис лицензирования СКЗИ.

Предварительные условия:

У пользователя есть устройство под управлением ОС Android и доступ к сети интернет.

Ну устройстве пользователя установлено МП Потребителя.

Выходные условия:

Приложение МП ЕБС установлено и настроено.

Инициирующее событие:

Решение пользователя обратиться в КО через ДКО (мобильное приложение) для получения услуги, требующей прохождения удаленной идентификации

Основной сценарий

Шаг 1. Пользователь запускает МП Потребителя БДн;

Шаг 2. Пользователь выбирает услугу КО, требующей прохождения удаленной идентификации

Шаг 3. МП Потребителя БДн вызывает функцию SDK проверки установленного МП ЕБС;

Шаг 4. МП Потребителя БДн предлагает пользователю установить МП ЕБС;

Шаг 5. Пользователь подтверждает свое согласие на установку МП ЕБС;

Шаг 6. МП Потребителя БДн переадресовывает пользователя на страницу распространения МП ЕБС в Google Play Market для загрузки приложения ЕБС;

Шаг 7. Пользователь загружает и устанавливает МП;

Шаг 8. Пользователь осуществляет первый запуск МП ЕБС;

Шаг 9. МП ЕБС предлагает Пользователю настроить приложение (отображает главный экран/экран входа в профиль с кнопкой "Войти через Госуслуги");
Шаг 10. Пользователь нажимает кнопку «Войти через Госуслуги»;
Шаг 11. МП ЕБС перенаправляет Пользователя на страницу авторизации ЕСИА (webview);
Шаг 12. Пользователь вводит логин/пароль от УЗ ЕСИА;
Шаг 13. ЕСИА авторизует пользователя и возвращает в МП ЕБС код авторизации;
Шаг 14. МП ЕБС обращается к ЕБС - сервису регистрации экземпляра МП, в параметрах запроса содержатся:

- код авторизации, полученный от ЕСИА;
- Instance ID.

Шаг 15. ЕБС обращается в ЕСИА за маркером доступа, предъявив полученный код авторизации;
Шаг 16. ЕБС извлекает из полученного маркера доступа ЕСИА OID УЗ пользователя;
Шаг 17. ЕБС формирует регистрационные данные пользователя и возвращает их в МП ЕБС:

- ID экземпляра мобильного приложения;
- ID пользователя

Шаг 18: МП ЕБС отображает Пользователю экран настройки библиотеки мобильного СКЗИ (троббер):
Шаг 18.1. МП ЕБС рассчитывает и сохраняет хэш-сумму сертификата, вносит доверенный сертификат TLS-шлюза в Хранилище доверенных сертификатов приложения;
Шаг 18.2. Библиотека рассчитывает контрольную сумму установки (контрольная сумма сохраняется и проверяется при каждом запуске МП для контроля целостности криптосредства и СФК);
Шаг 18.3. Библиотека обращается по URL сервера лицензий и передает регистрационные данные пользователя (наименование продукта, ID пользователя и контрольную сумму установки);
Шаг 18.4. МП ЕБС верифицирует сертификат сервера лицензий;
Шаг 18.5. Сервис лицензирования регистрирует экземпляр СКЗИ и возвращает положительный ответ в Библиотеку.

Шаг 20. МП ЕБС разблокирует прикладной режим работы и отображает пользователю экран с подтверждением готовности к работе в прикладном режиме (удаленная идентификация пользователя с использованием биометрии) и предлагает пользователю проверить корректность сертификата и контрольной суммы;

Шаг 21. МП ЕБС настроено и готово к работе.

Альтернативные сценарии

Шаг 1а. Пользователь устанавливает МП ЕБС напрямую из магазина приложений Google Play Market

Шаг 1а1. Переход на Шаг 8.

Шаг 3а. МП ЕБС уже установлено на мобильном устройстве пользователя

Шаг 3а.1. SDK запускаем МП ЕБС;

Шаг 20а. Пользователь не подтверждает корректность сертификата/контрольной суммы (Пользователь нажимает кнопку "Заблокировать и обновить" в разделе "Профиль"-"Настройки и безопасность"-"Проверить корректность сертификата")

Шаг 20а.1. МП ЕБС блокирует работу в прикладном режиме и отображает Пользователю экран с предложением обновить приложение или установить его заново. (экран содержит элемент перехода на страницу приложения в магазине приложений);

Шаг 20а.2. Пользователь обновляет (на странице приложения в магазине приложений нажимает "Обновить") и открывает заново МП ЕБС;

Шаг 20а.3. МП ЕБС предлагает Пользователю настроить приложение (отображает главный экран/экран входа в профиль с кнопкой "Войти через Госуслуги");

Шаг 20а.4. Пользователь нажимает кнопку «Войти через Госуслуги»;

Шаг 20а.5. МП ЕБС перенаправляет Пользователя на страницу авторизации ЕСИА (webview);

Шаг 20а.6. Пользователь вводит логин/пароль от УЗ ЕСИА;

Шаг 20а.7. ЕСИА авторизует пользователя и возвращает в МП ЕБС код авторизации;

Шаг 20а.8. МП ЕБС обращается к ЕБС - сервису регистрации экземпляра МП, в параметрах запроса содержатся:

- код авторизации, полученный от ЕСИА;
- Instance ID.

Шаг 20а.9. ЕБС обращается в ЕСИА за маркером доступа, предъявив полученный код авторизации;

Шаг 20а.10. ЕБС извлекает из полученного маркера доступа ЕСИА OID УЗ пользователя;

Шаг 20а.11. ЕБС формирует регистрационные данные пользователя и возвращает их в МП ЕБС:

- ID экземпляра мобильного приложения;
- ID пользователя.

Шаг 20а.12. МП ЕБС отображает Пользователю экран настройки библиотеки мобильного СКЗИ (троббер):

Шаг 20а.12.1 МП ЕБС рассчитывает хэш-сумму сертификата и проверяет, что сохраненная ранее хэш-сумма отклоненного сертификата не равна хеш-сумме сертификата в составе приложения;

Шаг 20а.12.2 МП ЕБС пересохраняет хэш-сумму сертификата и вносит сертификат в Хранилище доверенных сертификатов приложения.

Далее сценарий продолжается с Шаг 18.2 Основного сценария.

Шаг 20а.3а. На странице приложения в магазине приложений отсутствуют актуальные обновления

Шаг 20а.3а.1. Пользователь удаляет МП ЕБС с устройства

Далее сценарий продолжается с Шаг 1 Основного сценария.

Шаг 20а.6а. Проверка хэш-суммы обновленного и отклоненного сертификата не пройдена (сохраненная ранее хэш-сумма отклоненного сертификата равна хеш-сумме сертификата в составе приложения)

Шаг 20а.6а.1. МП ЕБС блокирует работу в прикладном режиме и отображает Пользователю экран с предложением обновить приложение или установить его заново. Экран содержит элемент перехода на страницу приложения в магазине приложений.

Далее сценарий продолжается с Шаг 20а.3а.1. Альтернативного сценария

Исключительные сценарии

Исключительный сценарий 1 - Пользователь не подтвердил установку МП ЕБС

Шаг 5а. Пользователь не подтвердил установку МП ЕБС

Шаг 5а.1 Сценарий завершается

Исключительный сценарий 2 – Пользователь не инициировал настройку МП ЕБС

Шаг 10а. Пользователь не инициировал настройку МП ЕБС

Шаг 10а.1 Сценарий завершается

Исключительный сценарий 3 – Пользователь не прошёл авторизацию ЕСИА

Шаг 13а Пользователь не прошёл авторизацию ЕСИА

Шаг 13а.1 Сценарий завершается

ПРИЛОЖЕНИЕ Г. Руководство пользователя по работе с библиотекой ЕБС.Sdk

1. Руководство пользователя по работе с библиотекой ЕБС.SDK для Android

1.1.Общее описание библиотеки

ЕБС.SDK представляет собой файл ru.rtlabs.mobile.ebs.sdk.aar. Для поддержки android.support используется файл ru.rtlabs.mobile.ebs.sdk.support.aar, который не требует подключения ru.rtlabs.mobile.ebs.sdk.aar.

Для авторизации в единой биометрической системе SDK предоставляет класс EbsApi из пакета ru.rtlabs.mobile.ebs.sdk.

При вызове метода requestEsiaAuthorization или requestEbsVerification, SDK проверяет наличие установленного на устройстве мобильного приложения ЕБС. В случае его отсутствия выводится диалоговое окно с запросом на установку МП ЕБС. При положительном ответе пользователя, если на устройстве установлено приложение Google Play Market, то в нем открывается окно приложения ЕБС, если приложение Google Play Market отсутствует, то открывается страница приложения ЕБС в Google Play Market в браузере.

Если приложение ЕБС установлено на устройстве, то после вызова requestEsiaAuthorization или requestEbsVerification открывается приложение ЕБС и начинается авторизация пользователя в ЕБС.

МП ЕБС производит процедуру получения биометрических образцов, которые передает в ЕБС на биометрическую верификацию пользователя. Результат биометрической верификации передается в пользовательское приложение. МП ЕБС возвращает интент с результатом в пользовательское приложение, который обрабатывается в onActivityResult. Интент содержит параметры результата верификации.

1.2.Описание классов

1.2.1. Класс EsiaAuthRequest

Класс EsiaAuthRequest представляет собой конфигурацию для запроса на авторизацию или получение расширенного результата ЕСИА в МП ЕБС, который передается в метод EbsApi.requestEsiaAuthorization.

1.2.1.1.Свойства класса EsiaAuthRequest:

Наименование свойства	Тип	Описание
infoSystem	String	Обязательный параметр. Возвращает идентификатор системы потребителя

Наименование свойства	Тип	Описание
esiaAuthUrl	String	Обязательный параметр. Возвращает url для авторизации в ЕСИА. Пример: «https://esia.gosuslugi.ru/aas/oauth2/ac?client_id=*&client_secret=*&scope=*&state=*&timestamp=*&redirect_uri=*&access_type=*&response_type=*» Вместо * ставиться соответствующее значение. В качестве scope используется «openi bio»

Для создания экземпляра класса EsiaAuthRequest используется EsiaAuthRequest.Builder. Если конфигурация EsiaAuthRequest не будет соответствовать требованиям, то МП ЕБС выведет сообщение: «Ошибка конфигурации процесса ЕСИА авторизации». Пример:

Пример:

```
EsiaAuthRequest esiaAuthRequest = new EsiaAuthRequest.Builder()
  .esiaAuthUrl("TEST_INFO_SYSTEM")

.esiaAuthUrl("https://esia.gosuslugi.ru/aas/oauth2/ac?client_id=*&client_secret=*&scope=*&state=*&timestamp=*&redirect_uri=*&access_type=*&response_type=*")
  .build();

EbsApi.requestEsiaAuthorization(context, esiaAuthRequest, ESIA_AUTH_REQUEST_CODE);
```

1.2.2. Класс EsiaAuthResult

Класс EsiaAuthResult представляет собой результат, который возвращает МП ЕБС пользовательскому приложению после авторизации или получения расширенного результата в ЕСИА.

1.2.2.1.Свойства класса EsiaAuthResult:

Наименование свойства	Тип	Описание
code	String	Возвращает code ЕСИА.
state	String	Возвращает state ЕСИА.

Наименование свойства	Тип	Описание
isEmpty	Boolean	Возвращает true если свойство code или state равно null или пустое
isNotEmpty	Boolean	Возвращает true если оба свойства code и state не null и не пустые

Для создания экземпляра класса *EsiaAuthResult* используется *EsiaAuthResult.Builder*. Результат авторизации в ЕСИА получается в *onActivityResult* методом *EbsApi.getEsiaAuthorizationResult(intent).* Полученные code и state используются для получения access_token ЕСИА и session_id верификации ЕБС.

Пример:

```
@Override
public void onActivityResult(int requestCode, int resultCode, Intent data) {

  if (requestCode == ESIA_AUTH_REQUEST_CODE &&
    resultCode == Activity.Result_OK) {

    EsiaAuthResult esiaAuthResult = EbsApi.getEsiaAuthorizationResult(data)
    if (esiaAuthResult.isNotEmpty()) {
      // Обработка положительного результата
    } else {
      // Обработка отрицательного результата
    }

  }


}
```

1.2.3. Класс VerificationRequest

Класс *VerificationRequest* представляет собой конфигурацию для запроса на верификацию в МП ЕБС, который передается в метод *EbsApi.requestEbsVerification*.

1.2.3.1.Свойства класса VerificationRequest:

Наименование свойства	Тип	Описание
infoSystem	String	Обязательный параметр. Возвращает идентификатор системы потребителя
sessionId	String	Обязательный параметр. Возвращает ИД сессии верификации в системе ЕБС

Для создания экземпляра класса *VerificationRequest* используется *VerificationRequest.Builder*. Если конфигурация *VerificationRequest* не будет соответствовать требованиям, то МП ЕБС выведет сообщение: «Ошибка конфигурации процесса верификации».

Пример:

```
VerificationRequest verificationRequest = new VerificationRequest.Builder()
  .infoSystem("TEST_INFO_SYSTEM")
  .sessionId("TEST_SESSION_ID")
  .build();

EbsApi.requestEbsVerification(context, verificationRequest,
VERIFICATION_REQUEST_CODE);
```

1.2.4. Класс VerificationResult

Класс *VerificationResult* представляет собой результат который возвращает МП ЕБС пользовательскому приложению после верификации в системе ЕБС.

1.2.4.1.Свойства класса VerificationResult:

Наименование свойства	Тип	Описание
resultCode	Int	Возвращает код результат, используется для дополнительных операция.

Наименование свойства	Тип	Описание
		Если *requestCode* == *EbsApi.REPEAT_RESULT_CODE*, то пользователь запрашивает повторное прохождение процесса авторизации, тогда пользовательское приложение должно заново инициировать прохождение авторизации с запроса на авторизацию в ЕСИА с новой сессией
verifyToken	String	Возвращает контрольное значение (уникальный идентификатор, созданный ЕБС для ЕСИА), необходимое для завершения процедуры аутентификации в ЕСИА после получения результата верификации.
expired	String	Возвращает время прекращения действия расширенного результата биометрической верификации пользователя в ЕСИА. Пример: «2018-07-20T04:50:19.981»
isEmpty	Boolean	Возвращает true если свойство verifyToken или expired равно null или пустое
isNotEmpty	Boolean	Возвращает true если свойства verifyToken и expired не равны null и не пустые одновременно.

Для создания экземпляра класса VerificationResult используется VerificationResult.Builder. Результат верификации в ЕБС получается в onActivityResult методом EbsApi.getEbsVerificationResult(intent).

Пример:

```
@Override
public void onActivityResult(int requestCode, int resultCode, Intent data) {

  if (requestCode == VERIFICATION_REQUEST_CODE &&
    resultCode == Activity.Result_OK) {

    VerificationResult verificationResult = EbsApi.getEbsVerificationResult (data)
```

```
    if (verificationResult.getResultCode() == EbsApi.REPEAT_RESULT_CODE) {
      // Старт повторной авторизации в ЕСИА
      // Необходимо создать новый esiaAuthRequest
      // EbsApi.requestEsiaAuthorization(context, esiaAuthRequest,
ESIA_AUTH_REQUEST_CODE);
    } else if (verificationResult.isNotEmpty()) {
      // Обработка положительного результата
    } else {
      // Обработка отрицательного результата
    }

  }


}
```

1.2.5. Класса EbsApi

Класс *EbsApi* предоставляет основные методы для взаимодействия пользовательского приложения и МП ЕБС.

1.2.5.1. Метод requestEsiaAuthorization(Activity context, EsiaAuthRequest request, int requestCode)

Основной метод, вызывает запрос на авторизацию или получение расширенного результата ЕСИА МП ЕБС в контексте android.app.Activity.

Параметры метода:

Наименование параметра	Тип параметра	Описание
context	android.app.Activity	Обязательный параметр. Контекст вызова. Если context == null, то бросается исключение IllegalArgumentException.
request	EsiaAuthRequest	Обязательный параметр. Конфигурация процесса авторизации ЕСИА. Если request == null, то бросается исключение IllegalArgumentException

Наименование параметра	Тип параметра	Описание
requestCode	int	Обязательный параметр. Код запроса, который используется в onActivityResult

Метод возвращает true, если приложение ЕБС обнаружено на устройстве и совершен переход в контекст приложения ЕБС, в других случаях возвращается false.

1.2.5.2. Метод requestEsiaAuthorization(Fragment context, EsiaAuthRequest request, int requestCode)

Основной метод, вызывает запрос на авторизацию или получение расширенного результата ЕСИА МП ЕБС в контексте android.app.Fragment.

Параметры метода:

Наименование параметра	Тип параметра	Описание
context	android.app.Fragment	Обязательный параметр. Контекст вызова. Если context == null или context.getActivity() == null, то бросается исключение IllegalArgumentException.
request	EsiaAuthRequest	Обязательный параметр. Конфигурация процесса авторизации ЕСИА. Если request == null, то бросается исключение IllegalArgumentException.
requestCode	int	Обязательный параметр. Код запроса, который используется в onActivityResult

Метод возвращает true, если приложение ЕБС обнаружено на устройстве и совершен переход в контекст приложения ЕБС, в других случаях возвращается false.

1.2.5.3.Метод getEsiaAuthorizationResult(Intent data)

Метод получает результат авторизации или получения расширенного результата ЕСИА в МП ЕБС типа *EsiaAuthResult* из объекта *Intent*.

Параметры метода:

Наименование параметра	Описание
data	Интент, полученный в *onActivityResult*, после выполнения запроса на авторизацию ЕСИА. Может быть null, тогда результат возвращается как *EsiaAuthResult* с пустыми полями.

Результат метода:

Объект класса *EsiaAuthResult*. При успешной авторизации в ЕСИА поля объекта не пустые и метод *IsNotEmpty* возвращает true, а *IsEmpty* – false. При не успешной авторизации в ЕСИА возвращается объект с пустыми полями, метод *IsNotEmpty* возвращает false, а *IsEmpty* – true.

1.2.5.4.Метод requestEbsVerification(Activity context, VerificationRequest request, int requestCode)

Основной метод, вызывает запрос на верификацию МП ЕБС в контексте *android.app.Activity*.

Параметры метода:

Наименование параметра	Тип параметра	Описание
context	android.app.Activity	Обязательный параметр. Контекст вызова. Если context == null, то бросается исключение IllegalArgumentException.
request	VerificationRequest	Обязательный параметр. Конфигурация процесса верификации ЕБС.

Наименование параметра	Тип параметра	Описание
		Если request == null, то бросается исключение IllegalArgumentException
requestCode	int	Обязательный параметр. Код запроса, который используется в onActivityResult

Метод возвращает true, если приложение ЕБС обнаружено на устройстве и совершен переход в контекст приложения ЕБС, в других случаях возвращается false.

1.2.5.5.Метод requestEbsVerification(Fragment context, VerificationRequest request, int requestCode)

Основной метод, вызывает запрос на верификацию МП ЕБС в контексте *android.app.Fragment.*

Параметры метода:

Наименование параметра	Тип параметра	Описание
context	android.app.Fragment	Обязательный параметр. Контекст вызова. Если context == null или context.getActivity() == null, то бросается исключение IllegalArgumentException.
request	VerificationRequest	Обязательный параметр. Конфигурация процесса верификации ЕБС. Если request == null, то бросается исключение IllegalArgumentException.
requestCode	int	Обязательный параметр. Код запроса, который используется в onActivityResult

Метод возвращает true, если приложение ЕБС обнаружено на устройстве и совершен переход в контекст приложения ЕБС, в других случаях возвращается false.

1.2.5.6.Метод getEbsVerificationResult(Intent data)

Метод получает результат верификации в системе ЕБС в МП ЕБС типа *VerificationResult* из объекта *Intent*.

Параметры метода:

Наименование параметра	Описание
data	Интент, полученный в *onActivityResult*, после выполнения запроса на авторизацию ЕСИА. Может быть null, тогда результат возвращается как *VerificationResult* с пустыми полями.

Результат метода:

Объект класса *VerificationResult*. При успешной авторизации в системе ЕБС поля объекта не пустые и метод *IsNotEmpty* возвращает true, а *IsEmpty* – false. При не успешной авторизации в ЕСИА возвращается объект с пустыми полями, метод *IsNotEmpty* возвращает false, а *IsEmpty* – true.

1.2.5.7.Схема работы

При вызове одного из метода *requestEsiaAuthorization* или *requestEbsVerification* ЕБС.SDK проверяет наличие установленного МП ЕБС на устройстве пользователя.

Если МП ЕБС установлено на устройстве пользователя, то ЕБС.SDK открывает МП ЕБС и начинается процесс авторизации ЕСИА или верификации ЕБС в зависимости от вызванного метода. ЕБС.SDK вызывает метод *startActivityForResult* переданного контекста пользовательского приложения, соответственно результат обрабатывается в *onActivityResult* переданного контекста.

Если МП ЕБС не установлено на устройстве пользователя, то открывается диалоговое окно с запросом у пользователя на установку МП ЕБС. Если пользователь отказывается, то диалоговое окно закрывается и процесс установки МП ЕБС заканчивается. Если пользователь соглашается на установку, то ЕБС.SDK проверяет наличие на устройстве Google Play Market, и если его обнаруживает, то открывается Google Play Market со страницей МП ЕБС. Если Google Play Market

не установлен на устройстве пользователя, то открывается веб ссылка на Google Play Market на страницу МП ЕБС.

1.2.5.8.Методы класса EbsApi из пакета ru.rtlabs.mobile.sdk.support

Если есть необходимость использовать android.support, то используется класс EbsApi из пакета ru.rtlabs.mobile.sdk.support. В данном классе помимо предыдущих методов, присутствуют методы requestAuthorization, где в качестве контекста передается *android.support.v4.app.Fragment*. А в качестве вывода диалогового окна запроса на установку МП ЕБС используется класс *android.support.v7.app.AlertDialog*.

1.3.Интеграция

Поместить файл SDK в папку проекта libs.

В build.gradle проекта прописать зависимости:

```
dependencies {
…

    implementation fileTree(dir: 'libs', include: ['*.jar', '*.aar'])

}
```

Также можно подключить через flatDir.

В корневом build.gradle прописываем:

```
allprojects {
        repositories {
         …

                flatDir {
              dirs 'libs'
         }
         }
}
```

В указанный dirs помещаем файл sdk. В build.gradle приложения:

```
dependencies {
        …

        implementation(name: 'ru.rtlabs.mobile.ebs.sdk', ext: 'aar') }

}
```

1.4.Зависимости

Библиотека ru.rtlabs.mobile.ebs.sdk.support зависит от com.android.support:appcompat-v7 и com.android.support:support-v4.

1.5.Пример использования

```
public class AuthActivity extends AppCompatActivity  {

  // Код запроса на авторизацию ЕСИА
  public static final int ESIA_AUTH_REQUEST_CODE = 101;
  // Код запроса на верификацию ЕБС
  public static final int VERIFICATION_REQUEST_CODE = 102;
  // Код запроса на получение расширенного результата
  public static final int ESIA_AUTH_RESULT_REQUEST_CODE = 103;

  // Метод, который стартует процесс авторизации пользователя
  public void onLogin() {
    startEsiaAuthRequest();
  }

  // Метод вызывает МП ЕБС для авторизации ЕСИА
  private void startEsiaAuthorizationRequest() {
    // Идентификатор системы
          String infoSystem = ...;
    // Пользовательское приложение формирует url для авторизации в ЕСИА
    String esiaAuthurl = ...;
    // Вызов авторизации ЕСИА в МП ЕБС
    EsiaAuthRequest esiaAuthRequest = new EsiaAuthRequest.Builder()
  .infoSystem(infoSystem)
        .esiaAuthUrl(esiaAuthUrl)
        .build();

    EbsApi.requestEsiaAuthorization(context, esiaAuthRequest,
ESIA_AUTH_REQUEST_CODE);
  }
  // Метод вызывает МП ЕБС для верификации ЕБС
  private void startEbsVerificationRequest(String infoSystem, String sessionId) {
    VerificationRequest verificationRequest = new VerificationRequest.Builder()
  .infoSystem(infoSystem)
  .sessionId(sessionId)
  .build();
```

```
    EbsApi.requestEbsVerification(context, verificationRequest,
VERIFICATION_REQUEST_CODE);
  }

  // Метод вызывает МП ЕБС для получения расширенного результата ЕСИА
  private void startEsiaAuthorizationResultRequest(VerificationResult result) {
    // Идентификатор системы
          String infoSystem = ...;
    // Пользовательское приложение формирует url для получения        расширенного
результата в ЕСИА
    String esiaAuthurl = ...;
    // Вызов авторизации ЕСИА в МП ЕБС
    EsiaAuthRequest esiaAuthRequest = new EsiaAuthRequest.Builder()
  .infoSystem(infoSystem)
        .esiaAuthUrl(esiaAuthUrl)
        .build();

    EbsApi.requestEsiaAuthorization(context, esiaAuthRequest,
ESIA_AUTH_RESULT_REQUEST_CODE);
  }

 @Override
public void onActivityResult(int requestCode, int resultCode, Intent data) {

  if (requestCode == ESIA_AUTH_REQUEST_CODE &&
    resultCode == Activity.Result_OK) {

    EsiaAuthResult esiaAuthResult = EbsApi.getEsiaAuthorizationResult(data)
    if (esiaAuthResult.isNotEmpty()) {
      // Обработка положительного результата
      // Пользовательское приложение обрабатывает результат
            // Пользовательское приложение получает ИД сессии верификации
      String sessionId = ...
      // Стартуем запрос на верификацию
      startEbsVerificationRequest(infoSystem, sessionId);
    } else {
      // Обработка отрицательного результата
    }

  } else if (requestCode == VERIFICATION_REQUEST_CODE &&
    resultCode == Activity.Result_OK) {

    VerificationResult verificationResult = EbsApi.getEbsVerificationResult (data)
```

```
    if (verificationResult.getResultCode() == EbsApi.REPEAT_RESULT_CODE) {
      // Старт повторной авторизации в ЕСИА
      startEsiaAuthRequest();
    } else if (verificationResult.isNotEmpty()) {
      startEsiaAuthorizationResultRequest(verificationResult)
    } else {
      // Обработка отрицательного результата
    }

  } else if (requestCode == ESIA_AUTH_RESULT_REQUEST_CODE) {
    EsiaAuthResult esiaAuthResult = EbsApi.getEsiaAuthorizationResult(data)
     if (esiaAuthResult.isNotEmpty()) {
      // Обработка положительного результата
    } else {
      // Обработка отрицательного результата
    }
  }


}


}
```

2. Руководство пользователя по работе с библиотекой ЕБС.SDK для iOS

2.1.Общее описание библиотеки

ЕБС.SDK представляет собой файл EbsSDK.framework.

Для авторизации в единой биометрической системе SDK предоставляет класс EbsSDKClient.

В первую очередь вызывает метод set(scheme: _), который конфигурирует SDK для работы с данным банковским приложением.

Затем после получения Location приложением банка вызывается метод requestEsiaSession(urlString: _) куда передается Location.

При вызове этого метода, SDK проверяет наличие установленного на устройстве мобильного приложения ЕБС. В случае его отсутствия выводится диалоговое окно с запросом на установку МП ЕБС. При положительном ответе пользователя открывается окно приложения ЕБС, если приложение отсутствует, то открывается приложение App Store с предложением установить МП ЕБС .

Если приложение ЕБС установлено на устройстве, то после вызова requestAuthorization в МП ЕБС производится авторизация пользователя в ЕСИА посредством логина/пароля.

После успешной авторизации в ЕСИА, результат ЕСИА авторизации передается в пользовательское приложение. МП ЕБС возвращает интент с результатом в пользовательское приложение, который обрабатывается в func application (_ app: UIApplication, open url: URL, options: [UIApplicationOpenURLOptionsKey : Any] = [:]) -> Bool

Ответ необходимо передать в handler. EbsSDKClient.shared.process(openUrl: url, from: options[UIApplicationOpenURLOptionsKey.sourceApplication]). Если авторизация прошла успешно, то SDK вернет State и Code. Используя их МП Банка должно получить SessionID для прохождения биоверификации пользователем. После успешного получения SessionID, вызывается метод requestAuthorization(sessionId: _)

МП ЕБС производит процедуру получения биометрических образцов, которые передает в ЕБС на биометрическую верификацию пользователя. Результат биометрической верификации передается в пользовательское приложение.

МП ЕБС возвращает url с результатом в пользовательское приложение, который обрабатывается в func application (_ app: UIApplication, open url: URL, options: [UIApplicationOpenURLOptionsKey : Any] = [:]) -> Bool

Ответ необходимо передать в handler. EbsSDKClient.shared.process(openUrl: url, from: options[UIApplicationOpenURLOptionsKey.sourceApplication])

2.2.Методы класса EbsSDKClient

2.2.1. Метод set(scheme: String, title: String, infoSystem: String, presenting controller: UIViewController)

Данный метод вызывается в самом начале и конфигурирует SDK.

Параметры метода:

Наименование параметра	Описание
scheme	Обязательный. URL-Schema, для которой МП-ЕБС вернет ответ приложению. Схема должны быть обязательно реализована в приложении Подробнее: https://developer.apple.com/library/content/documentation/iPhone/Conceptual/iPhoneOSProgrammingGuide/Inter-AppCommunication/Inter-AppCommunication.html

title	Заголовок окна авторизации в ЕСИА. Если title == nil, то заголовок окна используется по умолчанию
infoSystem	Обязательный. Инфосистема банка.
presenting controller	Обязательный. Передается объект UIViewController на котором происходит авторизация. Необходим для отображения алертов sdk.

2.2.2. Метод requestEsiaSession(urlString: String, completion: @escaping EsiaCompletion)

Метод отправляет запрос на получение Esia токена.

Параметры метода:

Наименование параметра	Описание
urlString	Обязательный. Строка Location, которая была получена в результате выполнения запроса «mob/rs/back/ac/session»
completion	Обязательный. Блок обработки результата авторизации. Структура enum EsiaRequestResult содержит 3 кейса: 1. success(esiaResult: EsiaToken). Содержит есиа токен в случае успешной авторизации a. code: String – код авторизации b. state: String – состояние вызова. 2. failure. - авторизация прошла неуспешно 3. cancel - авторизация прервана пользователем

Результат метода:

Результат метода приходит в блок completion. В случае успеха параметр не содержит ошибку и содержит токен. В случае неудачи – параметр блока содержит ошибку с описанием и не содержит токена.

2.2.3. Метод requestAuthorization(sessionId: String, completion: @escaping AuthorizationCompletion)

Метод вызывает запрос на получение токена ЕБС, путем прохождения биоверификации.

Параметры метода:

Наименование параметра	Описание
sessionId	Обязательный. Строка ID полученная в результате успешного выполнения запроса «mob/rs/back/session»
completion	Обязательный. Блок обработки результата авторизации. Структура enum AuthorizationRequestResult содержит 3 кейса: 1. success(token: EbsToken). Содержит токен в случае успешной авторизации a. verifyToken: String – токен b. expired: UInt64 – время жизни токена. 2. failure(error: AuthorizationError). Содержит токен в случае неудачной авторизации a. ebsNotInstalled – приложение Ebs не установлено b. identificationFailed - авторизация прошла неуспешно c. unknown - другая ошибка 3. cancel - авторизация прервана пользователем

Результат метода:

Результат метода приходит в блок completion. В случае успеха параметр не содержит ошибку и содержит токен. В случае неудачи – параметр блока содержит ошибку с описанием и не содержит токена.

2.2.4. Метод requestExtendedAuthorization(location: String, completion: @escaping EsiaCompletion)

Метод отправляет запрос на получение Esia токена для расширенной верификации.

Параметры метода:

Наименование параметра	Описание
urlString	Обязательный. Строка Location, которая была получена в результате выполнения запроса «mob/rs/back/ac/(sessionId)/result»

Completion	Обязательный. Блок обработки результата авторизации. Структура enum EsiaRequestResult содержит 3 кейса: 1. success(esiaResult: EsiaToken). Содержит есиа токен в случае успешной авторизации a. code: String – код авторизации b. state: String – состояние вызова. 2. failure. - авторизация прошла неуспешно 3. cancel - авторизация прервана пользователем

Результат метода:

Результат метода приходит в блок completion. В случае успеха параметр не содержит ошибку и содержит токен. В случае неудачи – параметр блока содержит ошибку с описанием и не содержит токена.

2.3.Интеграция

Допускается установка фреймворка без менеджера зависимостей. Подробнее: https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPFrameworks/Tasks/CreatingFrameworks.html#//apple_ref/doc/uid/20002258-106880

В AppDelegate необходимо импортировать библиотеку EbsSDK:

import EbsSDK

Также, в файле AppDelegate необходимо реализовать метод:

```
func application(_ app: UIApplication, open url: URL, options:
[UIApplicationOpenURLOptionsKey : Any] = [:]) -> Bool {
          EbsSDKClient.shared.process(openUrl: url, from:
options[UIApplicationOpenURLOptionsKey.sourceApplication] as! String)
         return true
        }
```

2.4.Зависимости

Приложение не использует дополнительные библиотеки для своей работы.

Для разрабатываемого приложения должен быть зарегистрирована URL-Scheme для возможности перехода в приложение с приложения МП ЕБС https://developer.apple.com/library/content/documentation/iPhone/Conceptual/iPhoneOSProgrammingGuide/Inter-AppCommunication/Inter-AppCommunication.html.

Для разрабатываемого приложения должен быть добавлен ключ в info.plist в LSApplicationQueriesSchemes с значением ebs.

2.5.Пример использования

```
EbsSDKClient.shared.set(scheme: «appdemo», title: «демо банк», infoSystem:
«test_info_system» presenting: self)
…

EbsSDKClient.shared.requestEsiaSession(urlString: locationString) { (result) in
                                        switch result {
                                        case .success(let esiaResult):
                                                …
                                        case .failure:
                                                …
                                        case .cancel:
                                                break
                                        }
                                }

…

        EbsSDKClient.shared.requestAuthorization(sessionId: sessionIdString) {
(result) in
                                        switch result {
                                        case .success(let ebsToken):
                                                                                …
                                        case .failure:
                                                                                …
                                        case .cancel:
                                              break
                                        }
                                }

…

        EbsSDKClient.shared.requestExtendedAuthorization(location: locationString,
completion: { (extendedResult) in
                                        guard let sSelf = self else { return }
                                        switch extendedResult {
                                        case .success(let esiaResult):
                                                break
                                        case .failure:
                                                                                …
                                        case .cancel:
                                                                                …
                                        }
```

```
})
```

ПРИЛОЖЕНИЕ Д. Руководство программиста по типовому решению информационной безопасности

1. Назначение документа

Полное наименование и условное обозначение системы: Программно-аппаратный комплекс электронной подписи биометрических данных при подключении к Единой биометрической системе.

Условное обозначение: Адаптер, Система.

Целью создания Системы является обеспечение возможности для КО проведения удаленной электронной биометрической верификации пользователей по биометрическим характеристикам (далее удаленная идентификация) для исполнения требований, установленных Федеральным законом № 115-ФЗ, Федеральным законом № 149-ФЗ и размещения или обновления в Единой биометрической системе биометрических персональных данных (далее – регистрация БО).

Разработанный Адаптер к ЕСИА и ЕБС реализует необходимые протоколы обмена с ЕСИА и ЕБС, обеспечивает формирование и проверку ЭП в части взаимодействия с ЕСИА, ЕБС, СМЭВ, что упрощает для КО 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 идентификация с использованием ЕБС;
- формирование пакетов данных СМЭВ для передачи БО в ЕБС;
- интеграцию с HSM разных производителей для безопасного хранения и использования секретных ключей электронной подписи (отечественные криптографические алгоритмы);
- поддержку отечественных криптографических алгоритмов в части взаимодействия по протоколу TLS;
- простой API для интеграции с ИС КО.

Адаптер позволяет реализовать КО 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, подлежащих автоматизации, Адаптер выполняет следующие группы (комплексы) функций:

- группа функций процесса удаленной идентификации для решения задачи работы в рамках протокола OpenId Connect со стороны клиента (банка, проводящего авторизацию пользователя с использованием его биометрических данных - удаленную идентификацию) (внутренний API верификации Адаптера);
- группа функций процесса удаленной идентификации для решения задачи работы в рамках протокола OpenId Connect со стороны пользователя (внешний API верификации Адаптера);
- группа функций получения результата верификации для ДБО КО (API получения результата верификации ДБО КО);
- 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 управления, журналирования и мониторинга.

Группа функций управления, журналирования и мониторинга является вспомогательной и обеспечивает управление компонентами Адаптера и контроль их работоспособности.

2. Состав программных компонентов

СПО функционирует под управлением Java-машины и исполняется на ОС, которая соответствует Руководящим документам ФСТЭК для СВТ по 3 классу и Руководящим документам ФСТЭК по НДВ по 2 уровню, либо требованиям ФСБ России по защите конфиденциальной информации от несанкционированного доступа в автоматизированных информационных системах по классу АК3. Данные ОС и Java-машина являются покупными программными средствами:

- ОС "Astra Linux Special Edition". Релиз "Смоленск";
- ГосJava, коммерческая версия (специальная версия Java для работы в операционных системах "Astra Linux Special Edition" и "Альт Линукс СПТ");
- CryptoPro Java CSP 5.0.

Реализацию криптографических операций формирования и проверки электронной подписи обеспечивает HSM (СКЗИ класса КВ2).

СПО использует сторонние библиотеки, ПО (кроме перечисленных в разделе 4.1 покупных программных средств) только с открытым исходным кодом и поставляемых на условиях лицензий:

- не требующих раскрытия исходных кодов приложения;
- не требующих выпускать приложение под той же лицензией;
- не требующих распространять исходный код вместе с продуктом;

– разрешающих коммерческое использование, распространение, изменение.

СПО использует СУБД Postgresql 9.5 (входит в состав покупного программного средства ОС "Astra Linux Special Edition") для сохранения сессионной информации процесса удаленной идентификации.

СПО использует контейнер сервлетов Apache Tomcat (входят в состав покупного программного средства ГосJava, коммерческая версия) для исполнения модулей Системы.

СПО использует покупное программное средство CryptoPro Java CSP 5.0 для взаимодействия с клиентом HSM.

3. Описание интерфейсов доступа

Требования к схеме взаимодействий со смежными системами и используемых при обмене API в рамках процессов удаленной идентификации и регистрации БО приведена на рисунке ниже (Рисунок 11).

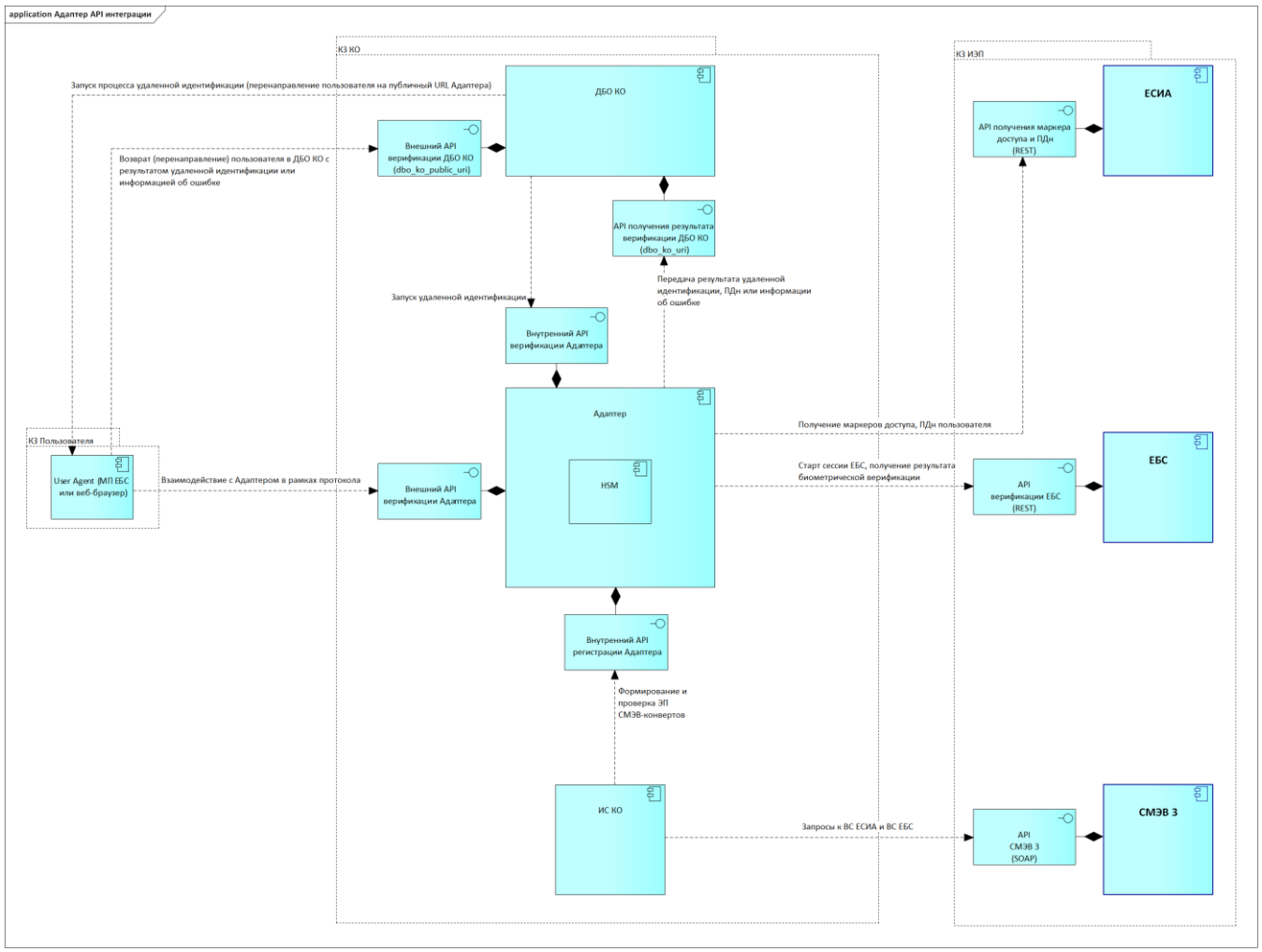

Рисунок 11 Схема взаимодействия со смежными системами и используемых при обмене API в рамках процессов удаленной идентификации и регистрации БО

Адаптер предоставляет смежным системам следующие API:

– Внутренний API верификации Адаптера. Доступен для вызовов только из ДБО КО в

пределах контролируемой зоны КО. Описание API приведено в разделе 3.4;

- Внешний API верификации Адаптера. Доступен для вызовов из сети Интернет. Описание API приведено в разделе 3.5;
- Внутренний API регистрации Адаптера. Доступен для вызовов только из ИС КО в пределах контролируемой зоны КО. Описание API приведено в разделе 3.8.

Для взаимодействия с Адаптером в рамках протокола удаленной идентификации ДБО КО реализует следующие API:

- API получения результата верификации ДБО КО. Доступен для вызовов только из Адаптера в пределах контролируемой зоны КО. Описание API приведено в разделе 3.6;
- Внешний API верификации ДБО КО. Доступен для вызовов из сети Интернет. Описание API приведено в разделе 3.7.

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.

3.1.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.

Актуальная версия API: «v1».

Формат версии: префикс «v» и целое число.

3.2.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»):

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

Входные параметры метода передаются в виде строки запроса[36] (часть URL после знака «?», разделитель параметров — знак «&») с передаваемыми на сервер параметрами при

36 Согласно RFC 3986, раздел 3.4

использовании метода GET, либо в теле POST-запроса. В случае GET-запроса, параметры должны быть закодированы с помощью URL Encoding[37], 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[38].

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 каждый входной параметр метода 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;
- заголовочное поле «Content-Type», принимающее значение в зависимости от контента, передаваемого в части:
  - входные параметры функции (см. раздел 3.8.1): «application/xml»;
  - биометрический образец: в зависимости от MIME типа вложения - биометрического образца, регистрируемого в ЕБС (см. раздел 3.8.1).

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 для конкретного метода. Текстовые значения параметров передаются в кодировке UTF-8.

3.3.Используемые в API Адаптера коды ответов HTTP

Предоставляемые Адаптером смежным системам API используют коды ответов HTTP, 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.)

37 Согласно RFC 3986, раздел 2.1

38 Согласно RFC 7159

Код ответа	Примечания
500 Internal Server Error	Вызов метода завершился с ошибкой на стороне сервера (ЕБС). Код ошибки включен в HTTP BODY.

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 (ДБО КО и ИС КО):

- 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 ДБО КО код ошибки и ее описание (см. раздел 3.6.1);
- перенаправляет пользователя на внешний API верификации ДБО КО (доступный из сети Интернет) URL ДБО КО (см. раздел 3.7).

3.4.Внутренний API верификации Адаптера

Используется ДБО КО для старта процесса аутентификации с использованием ЕСИА и ЕБС. Вызовы осуществляются в пределах контролируемой зоны КО.

Аспект реализации	Реализация
Транспортный протокол	HTTPS
Аутентификация вызывающей стороны	Authorization - обязательный заголовок в запросе.

Аспект реализации	Реализация
	Имеет вид Authorization: Bearer токен_доступа. Токен доступа прописывается в конфигурации Адаптера и выдается ППО ДБО КО.

3.4.1. Функция "Создание сессии в Адаптере"

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

3.5.Внешний API верификации Адаптера

Используется пользователем (браузер или мобильное приложение) для аутентификации с использованием ЕСИА и ЕБС.

Взаимодействие осуществляется по защищенному каналу (HTTPS с российскими или, опционально, зарубежными криптографическими алгоритмами. HTTPS терминируется на TLS-шлюзе Адаптера.

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

3.5.1. Функция "Запрос пользователя на начало аутентификации"

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

Успешным ответом является возврат вызывающей стороне сформированного запроса для перенаправления на ЕСИА с целью аутентификации пользователя.

Выходные параметры

Параметр	Тип данных	Обязательность	Описание
client_id	Строка	Да	Мнемоника Адаптера КО, зарегистрированная в ЕСИА
scope	Строка	Да	Константа: "openid, bio"
state	Строка	Да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID.
redirect_uri	Строка	Да	Ссылка, по которой ЕСИА должна направить пользователя после того, как он авторизуется в ЕСИА и даст разрешение на доступ к областям доступа (параметр scope)
cookie	Строка	Да	Идентификатор сессии клиента. Передается в заголовке ответа "Set-Cookie".

Прикладные ошибки

Ошибка	Код	Описание
Сессия не существует		Сессия sid не существует
Неверные параметры запроса		Неверные параметры запроса

3.5.2. Функция "Получение доступа к биометрической верификации"

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.

Входные параметры

Параметр	Тип данных	Обязательность	Описание
auth_code	Строка base64	Да	Код авторизации code1 для scope=«openid, bio»
state	Строка	Да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID.

Параметр	Тип данных	Обязательность	Описание
cookie	Строка	Да	Идентификатор сессии клиента. Передается в заголовке запроса «Cookie».

Успешный ответ

В случае успешного ответа возвращается сообщение, содержащее URL веб-формы и идентификатор сессии в ЕБС для перенаправления клиента с целью проведения биометрической верификации пользователя.

Ошибки

Ошибка	Код	Описание
Сессия не существует		Сессия cookie не существует
Неверный state		Неверный параметр state
Неверные параметры запроса		Неверные параметры запроса
Недействительный код авторизации		Ошибка проверки кода авторизации

3.5.3. Функция "Передача результата верификации"

Вызывается пользователем после прохождения биометрической верификации в ЕБС.

Входные параметры

Параметр	Тип данных	Обязательность	Описание
verify_token	Строка	Нет	Присутствует, в случае успешного прохождения пользователем биометрической верификации. Контрольное значение (уникальный идентификатор, созданный ЕБС для ЕСИА), необходимое для завершения процедуры аутентификации в ЕСИА после получения результата верификации.
expired	Число	Нет	Присутствует, в случае успешного прохождения пользователем биометрической верификации. Время прекращения действия результата биометрической верификации пользователя в ЕСИА, в миллисекундах с 1 января 1970 г. 00:00:00 GMT. После указанного в параметре момента времени получение специального маркера доступа со скоупом ext_auth_result в ЕСИА будет невозможно.
state	Строка	Да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID.
cookie	Строка	Да	Идентификатор сессии клиента. Передается в заголовке запроса "Cookie".

Успешный ответ

Успешным ответом является возврат вызывающей стороне (клиенту) сформированного запроса для перенаправления на ЕСИА с целью аутентификации пользователя.

Выходные параметры

Параметр	Тип данных	Обязательность	Описание
client_id	Строка	Да	Мнемоника Адаптера КО, зарегистрированная в ЕСИА
scope	Строка	Да	Константа: "openid, ext_auth_result"
state	Строка	Да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID
verify_token	Строка	Нет	Присутствует, в случае успешного прохождения пользователем биометрической верификации. Контрольное значение (уникальный идентификатор, созданный ЕБС для ЕСИА), необходимое для завершения процедуры аутентификации в ЕСИА после получения результата верификации.

Прикладные ошибки

Ошибка	Код	Описание
Сессия не существует		Сессия cookie не существует
Неверный state		Неверный параметр state
Неверные параметры запроса		Неверные параметры запроса
Время прекращения действия результата превышено		Время действия результата биометрической верификации пользователя в ЕСИА превышено

3.5.4. Функция "Получение специального параметра завершения протокола"

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

Входные параметры

Параметр	Тип данных	Обязательность	Описание
auth_code	Строка base64	Да	Код авторизации code2 для scope="openid, ext_auth_result"
state	Строка	Да	Набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID.
cookie	Строка	Да	Идентификатор сессии клиента. Передается в заголовке запроса "Cookie".

Успешный ответ

Выходные параметры

Параметр	Тип данных	Обязательность	Описание
res_secret	Строка base64	Нет	Присутствует только в случае успешного прохождения пользователем протокола проведения идентификации и аутентификации пользователя, запрашивающего доступ к ресурсам КО. Параметр, с использованием которого далее происходит взаимодействие пользователя и КО

Ошибки

Ошибка	Код	Описание
Сессия не существует		Сессия cookie не существует
Неверный state		Неверный параметр state
Неверные параметры запроса		Неверные параметры запроса
Недействительный код авторизации		Ошибка проверки кода авторизации

3.6.Спецификация API получения результата верификации ДБО КО

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

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

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

Прикладные ошибки, которые Адаптер может вернуть в ДБО КО:

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

Значение параметра «code»	Описание (параметр «message»)
ADR-0211	Получено сообщение об ошибке от ЕБС
ADR-0212	Ошибка формата данных полученных из ЕБС

3.6.1. Функция "Получение результата удаленной идентификации"

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

Адаптер осуществляет вызов на URL, переданный ДБО КО в параметре dbo_ko_uri при вызове функции Адаптера "Создание сессии в Адаптере".

Поддерживаемый метод HTTP запроса:

```
POST
```

URL запроса к данной функции API ДБО КО:

```
{{dbo_ko_uri}}
```

Где,

{{dbo_ko_uri}} - URL "API получения результата верификации ДБО КО", который был передан Адаптеру от ДБО КО при вызове функции "Создание сессии в Адаптере" (см. раздел 3.4.1) 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.

Параметр	Тип данных	Обязательность	Описание
			Присутствует только в случае успешного прохождения пользователем процесса удаленной идентификации с использованием ЕСИА и ЕБС. Параметр, с использованием которого далее происходит взаимодействие пользователя и КО
extended_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.
user_data	Массив	Нет	Необязательный параметр. Присутствует только в случае успешного прохождения пользователем процесса удаленной идентификации с использованием ЕСИА и ЕБС. Полученные из ЕСИА ПДн пользователя.

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",
  "extended_result": "
eyJraWQiOiIyNTE4ZDNhMy05NTc0LTRkOTMtODQ0YS0wZjIwNjE2YTI3MjQiLCJ0eXAiOiJKV1QiLCJhb
```

```
GciOiJHT1NUMzQxMCJ9.eyJyZXN1bHQiOnRydWUsInN1YiI6IjEwMDAzMTY5MTEiLCJhdWQiOiJUS19VQ
lNfREVWIiwibmJmIjoxNTUzMDAxNjgxLCJpc3MiOiJVQlNfREVWIiwibWF0Y2giOiJ7XCJvdmVyYWxsXC
I6MS4wLFwiZmFjZVwiOjEuMCxcInZvaWNlXCI6MS4wfSIsImV4cCI6MTU1MzAwMjI4MiwiaWF0IjoxNTU
zMDAxNjgwfQ==.BxQtSa5H7xpEZ_n8xiyy1F1D-
RiQDCDFGnucN6GCkmBKOwY0AxxNEl8TTN9wLNoYGBcEmD1RPNQhrDe45pHFgA==",
  "user_data": {
    "firstName": "ПФЛБфамилия",
    "lastName": "ПФЛБимя",
    "middleName": "ПФЛБотчество",
    "gender": "M",
    "citizenship": "RUS",
    "snils": "020-111-594 68"
  }
}
```


Пример ответа ДБО КО:

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

Прикладные ошибки на стороне ДБО КО (реализует ДБО КО):

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

3.7.Спецификация внешнего API верификации ДБО КО

ДБО КО должен реализовать функцию данного API. Вызовы функции осуществляются из сети Интернет от User Agent пользователя.

3.7.1. Функция "Возврат пользователя в ДБО КО"

Функция используется Адаптером для перенаправления (возврата) User Agent пользователя в ДБО КО 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 ДБО КО в параметре dbo_ko_public_uri при вызове функции Адаптера "Создание сессии в Адаптере".

В случае успешного выполнения протокола, в ДБО КО передается результат удаленной идентификации, ПДн пользователя, специальный параметр "res_secret", который пользователь предъявляет ДБО КО для выполнения бизнес-операции в ДБО КО 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 ДБО КО код и описание ошибки (см. раздел 3.6, функция "Получение результата удаленной идентификации"). Затем Адаптер перенаправляет пользователя на публичный URL, переданный ДБО КО в параметре dbo_ko_public_uri.

Заголовок Location:

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

Где,

{{sid}} - идентификатор сессии пользователя.

Пример запроса (перенаправления пользователя на dbo_ko_public_uri), если удаленная идентификация завершилась с ошибкой и код ошибки был успешно передан в ДБО КО (см. раздел 3.6):

```
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 ДБО КО (см. раздел 3.6, 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.

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

Пример запроса (перенаправления пользователя на dbo_ko_public_uri), если удаленная идентификация завершилась с ошибкой и код ошибки не был передан в ДБО КО (ДБО КО 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 ДБО КО.

3.8.Внутренний API регистрации Адаптера

API используется ДБО КО 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 КО.

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 ДБО КО.

3.8.1. 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 КО 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 КО), подписывается ЭП в формате XML Dsig (Адаптер формирует блок ЭП " CallerInformationSystemSignature").
- готовый к отправке (подписанный ЭП) блок "SendRequestRequest" возвращается ИС КО.

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 КО) подписывается ЭП в формате XML Dsig (Адаптер формирует блок ЭП " CallerInformationSystemSignature")
- готовый к отправке (подписанный ЭП) блок "AckRequest" возвращается ИС КО.

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 КО) подписывается ЭП в формате XML Dsig (Адаптер формирует блок ЭП " CallerInformationSystemSignature");
- готовый к отправке (подписанный ЭП) блок "GetResponseRequest" возвращается ИС КО.

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
```

Заголовки запроса:

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

Где,

{{token}} - токен доступа ИС КО 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(блок "SendRequestRequest")

Пример запроса:

```
POST /api/v1/reg/sign HTTP/1.1
Authorization: Bearer FAEA055D4EE948CEA031ACE10ECDAE49
Content-Length: 2297
Content-Type: multipart/form-data; boundary=--------------------------
fdeab0142d9d



------------------------------fdeab0142d9d
Content-Disposition: form-data; name="xml_payload"
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<SendRequestRequest xmlns="urn://x-artefacts-smev-gov-ru/services/message-
exchange/types/1.2" xmlns:ns2="urn://x-artefacts-smev-gov-ru/services/message-
exchange/types/basic/1.2"
                    xmlns:ns3="urn://x-artefacts-smev-gov-ru/services/message-
exchange/types/faults/1.2">
  <SenderProvidedRequestData Id="SIGNED_BY_CALLER">
    <MessageID>1a6d6f57-b7e6-11e7-be0f-3c5282dbde86</MessageID>
    <ReferenceMessageID>1a6d6f57-b7e6-11e7-be0f-3c5282dbde86</ReferenceMessageID>
    <ns2:MessagePrimaryContent>
      <RegisterBiometricDataRequest:RegisterBiometricDataRequest xmlns="urn://x-
artefacts-nbp-rtlabs-ru/register/1.2.0"

xmlns:RegisterBiometricDataRequest="urn://x-artefacts-nbp-rtlabs-
ru/register/1.2.0">
        <RegistrarMnemonic>TEST01</RegistrarMnemonic>
        <BiometricData>
                <Id>ID-1</Id>
                <Date>2017-07-31T16:54:52+03:00</Date>
                <RaId>0c2c345f-cd7b-4011-9f3b-65095ab4c186</RaId>
                <PersonId>240631324</PersonId>
                <IdpMnemonic>ESIA</IdpMnemonic>
```

```
                <Data>
                        <Modality>SOUND</Modality>
                        <AttachmentRef attachmentId="4fa53dd4-ca7d-4361-a736-
c935dcfae943"/>
                        <BioMetadata>
                                <Key>Voice_1_start</Key>
                                <Value>00.000</Value>
                                <Key>Voice_1_end</Key>
                                <Value>10.002</Value>
                                <Key>Voice_1_desc</Key>
                                <Value>digits_asc</Value>
                                <Key>Voice_2_start</Key>
                                <Value>12.601</Value>
                                <Key>Voice_2_end</Key>
                                <Value>20.199</Value>
                                <Key>Voice_2_desc</Key>
                                <Value>digits_desc</Value>
                                <Key>Voice_3_start</Key>
                                <Value>22.001</Value>
                                <Key>Voice_3_end</Key>
                                <Value>30.102</Value>
                                <Key>Voice_3_desc</Key>
                                <Value>digits_random</Value>
                        </BioMetadata>
                </Data>
                <Data>
                        <Modality>PHOTO</Modality>
                        <AttachmentRef attachmentId="b4582676-e6ae-497c-a60c-
27feb8525e84"/>
                </Data>
        </BiometricData>
      </RegisterBiometricDataRequest:RegisterBiometricDataRequest>
    </ns2:MessagePrimaryContent>
    <BusinessProcessMetadata />
  </SenderProvidedRequestData>
</SendRequestRequest>

------------------------------fdeab0142d9d
Content-Disposition: form-data; name="b4582676-e6ae-497c-a60c-27feb8525e84";
filename="sign-test1.jpeg"
```

```
Content-Type: image/jpeg

{{Бинарное содержимое файл фото лица}}
------------------------------fdeab0142d9d
Content-Disposition: form-data; name="4fa53dd4-ca7d-4361-a736-c935dcfae943";
filename="sign-test2.wav"
Content-Type: audio/pcm

{{Бинарное содержимое файла аудиозаписи голоса}}
------------------------------fdeab0142d9d--
```

Пример ответа:

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

<?xml version="1.0" encoding="UTF-8" standalone="no"?><SendRequestRequest
xmlns="urn://x-artefacts-smev-gov-ru/services/message-exchange/types/1.2"
xmlns:ns2="urn://x-artefacts-smev-gov-ru/services/message-
exchange/types/basic/1.2" xmlns:ns3="urn://x-artefacts-smev-gov-
ru/services/message-exchange/types/faults/1.2">
  <SenderProvidedRequestData Id="SIGNED_BY_CALLER">
    <MessageID>1a6d6f57-b7e6-11e7-be0f-3c5282dbde86</MessageID>
    <ReferenceMessageID>1a6d6f57-b7e6-11e7-be0f-3c5282dbde86</ReferenceMessageID>
    <ns2:MessagePrimaryContent>
      <RegisterBiometricDataRequest:RegisterBiometricDataRequest xmlns="urn://x-
artefacts-nbp-rtlabs-ru/register/1.2.0"
xmlns:RegisterBiometricDataRequest="urn://x-artefacts-nbp-rtlabs-
ru/register/1.2.0">
        <RegistrarMnemonic>TEST01</RegistrarMnemonic>
        <BiometricData>
                <Id>ID-1</Id>
                <Date>2017-07-31T16:54:52+03:00</Date>
                <RaId>0c2c345f-cd7b-4011-9f3b-65095ab4c186</RaId>
                <PersonId>240631324</PersonId>
                <IdpMnemonic>ESIA</IdpMnemonic>
                <Data>
                        <Modality>SOUND</Modality>
                        <AttachmentRef attachmentId="4fa53dd4-ca7d-4361-a736-
c935dcfae943"/>
                        <BioMetadata>
```

```
                                <Key>Voice_1_start</Key>
                                <Value>00.000</Value>
                                <Key>Voice_1_end</Key>
                                <Value>10.002</Value>
                                <Key>Voice_1_desc</Key>
                                <Value>digits_asc</Value>
                                <Key>Voice_2_start</Key>
                                <Value>12.601</Value>
                                <Key>Voice_2_end</Key>
                                <Value>20.199</Value>
                                <Key>Voice_2_desc</Key>
                                <Value>digits_desc</Value>
                                <Key>Voice_3_start</Key>
                                <Value>22.001</Value>
                                <Key>Voice_3_end</Key>
                                <Value>30.102</Value>
                                <Key>Voice_3_desc</Key>
                                <Value>digits_random</Value>
                        </BioMetadata>
                </Data>
                <Data>
                        <Modality>PHOTO</Modality>
                        <AttachmentRef attachmentId="b4582676-e6ae-497c-a60c-
27feb8525e84"/>
                </Data>
        </BiometricData>
      </RegisterBiometricDataRequest:RegisterBiometricDataRequest>
    </ns2:MessagePrimaryContent>
    <ns2:RefAttachmentHeaderList><ns2:RefAttachmentHeader><ns2:uuid>b4582676-
e6ae-497c-a60c-
27feb8525e84</ns2:uuid><ns2:Hash>t57W10FV3nFxv8dNvi7kVTu1z/eJ0Izh4aXd1EawpQ0=</ns
2:Hash><ns2:MimeType>image/jpeg</ns2:MimeType><ns2:SignaturePKCS7>MIIEzgYJKoZIhvc
NAQcCoIIEvzCCBLsCAQExDDAKBgYqhQMCAgkFADALBgkqhkiG9w0BBwGgggMwMIIDLDCCAtugAwIBAgIT
EgAwNDssYSeHmqR66gAAADA0OzAIBgYqhQMCAgMwfzEjMCEGCSqGSIb3DQEJARYUc3VwcG9ydEBjcnlwd
G9wcm8ucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxFzAVBgNVBAoTDkNSWVBUTy1QUk8gTE
xDMSEwHwYDVQQDExhDUllQVE8tUFJPIFRlc3QgQ2VudGVyIDIwHhcNMTgxMjEyMTMyNTA5WhcNMTkwMzE
yMTMzNTA5WjA+MRAwDgYDVQQDDAdteV90ZXN0MQ8wDQYDVQQKDAZSVExhYnMxGTAXBgkqhkiG9w0BCQEW
CnRlc3RAdHMucnUwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUDAgIeAQNDAARALSydgtZTKw9ECi+2F
UqL90Yn5y+hKuGkCDjGwar2AzbdWUOm8WIjEFEtQHjON7wHS1w8koXvxHJ9jr6zFvCN2qOCAW0wggFpMB
MGA1UdJQQMMAoGCCsGAQUFBwMEMAsGA1UdDwQEAwIGwDAdBgNVHQ4EFgQUZ7oyl4Vjj4M3FQ+P29yp7Lf
```

4h10wHwYDVR0jBBgwFoAUFTF8sI0a3mbXFZxJUpcXJLkBeoMwWQYDVR0fBFIwUDBOoEygSoZIaHR0cDov
L3Rlc3RjYS5jcnlwdG9wcm8ucnUvQ2VydEVucm9sbC9DUllQVE8tUFJPJTIwVGVzdCUyMENlbnRlciUyM
DIuY3JsMIGpBggrBgEFBQcBAQSBnDCBmTBhBggrBgEFBQcwAoZVaHR0cDovL3Rlc3RjYS5jcnlwdG9wcm
8ucnUvQ2VydEVucm9sbC90ZXN0LWNhLTIwMTRfQ1JZUFRPLVBSTyUyMFRlc3QlMjBDZW50ZXIlMjAyLmN
ydDA0BggrBgEFBQcwAYYoaHR0cDovL3Rlc3RjYS5jcnlwdG9wcm8ucnUvb2NzcC9vY3NwLnNyZjAIBgYq
hQMCAgMDQQAoeTnuXVpWLiCG052JlgkFsmD9g/nxgoPpTmj4W1YrS7b6I+0f4RM/IuJbcD7+vM25L5mxN
Bc8ozvEh5PkP83lMYIBZTCCAWECAQEwgZYwfzEjMCEGCSqGSIb3DQEJARYUc3VwcG9ydEBjcnlwdG9wcm
8ucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxFzAVBgNVBAoTDkNSWVBUTy1QUk8gTExDMSE
wHwYDVQQDExhDUllQVE8tUFJPIFRlc3QgQ2VudGVyIDICExIAMDQ7LGEnh5qkeuoAAAAwNDswCgYGKoUD
AgIJBQCgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0xOTAzMjExNDA3N
TVaMC8GCSqGSIb3DQEJBDEiBCC3ntbXQVXecXG/x02+LuRVO7XP94nQjOHhpd3URrClDTAKBgYqhQMCAh
MFAARATGsy78JQJECy/YrApmjtD2dyPTzUga7/4HI7RcXpNS1Kw2jw5KZD1U7MBULAAvqJLj8QTxCZeD5
jnmoyKxpZFA==</ns2:SignaturePKCS7></ns2:RefAttachmentHeader><ns2:RefAttachmentHea
der><ns2:uuid>4fa53dd4-ca7d-4361-a736-
c935dcfae943</ns2:uuid><ns2:Hash>HtdcUlvOLhRqnbT7wRoX3Jy7pSOeqRZqe7lMaoQMaXo=</ns
2:Hash><ns2:MimeType>audio/pcm</ns2:MimeType><ns2:SignaturePKCS7>MIIEzgYJKoZIhvcN
AQcCoIIEvzCCBLsCAQExDDAKBgYqhQMCAgkFADALBgkqhkiG9w0BBwGgggMwMIIDLDCCAtugAwIBAgITE
gAwNDssYSeHmqR66gAAADA0OzAIBgYqhQMCAgMwfzEjMCEGCSqGSIb3DQEJARYUc3VwcG9ydEBjcnlwdG
9wcm8ucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxFzAVBgNVBAoTDkNSWVBUTy1QUk8gTEx
DMSEwHwYDVQQDExhDUllQVE8tUFJPIFRlc3QgQ2VudGVyIDIwHhcNMTgxMjEyMTMyNTA5WhcNMTkwMzEy
MTMzNTA5WjA+MRAwDgYDVQQDDAdteV90ZXN0MQ8wDQYDVQQKDAZSVExhYnMxGTAXBgkqhkiG9w0BCQEWC
nRlc3RAdHMucnUwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUDAgIeAQNDAARALSydgtZTKw9ECi+2FU
qL90Yn5y+hKuGkCDjGwar2AzbdWUOm8WIjEFEtQHjON7wHS1w8koXvxHJ9jr6zFvCN2qOCAW0wggFpMBM
GA1UdJQQMMAoGCCsGAQUFBwMEMAsGA1UdDwQEAwIGwDAdBgNVHQ4EFgQUZ7oyl4Vjj4M3FQ+P29yp7Lf4
h10wHwYDVR0jBBgwFoAUFTF8sI0a3mbXFZxJUpcXJLkBeoMwWQYDVR0fBFIwUDBOoEygSoZIaHR0cDovL
3Rlc3RjYS5jcnlwdG9wcm8ucnUvQ2VydEVucm9sbC9DUllQVE8tUFJPJTIwVGVzdCUyMENlbnRlciUyMD
IuY3JsMIGpBggrBgEFBQcBAQSBnDCBmTBhBggrBgEFBQcwAoZVaHR0cDovL3Rlc3RjYS5jcnlwdG9wcm8
ucnUvQ2VydEVucm9sbC90ZXN0LWNhLTIwMTRfQ1JZUFRPLVBSTyUyMFRlc3QlMjBDZW50ZXIlMjAyLmNy
dDA0BggrBgEFBQcwAYYoaHR0cDovL3Rlc3RjYS5jcnlwdG9wcm8ucnUvb2NzcC9vY3NwLnNyZjAIBgYqh
QMCAgMDQQAoeTnuXVpWLiCG052JlgkFsmD9g/nxgoPpTmj4W1YrS7b6I+0f4RM/IuJbcD7+vM25L5mxNB
c8ozvEh5PkP83lMYIBZTCCAWECAQEwgZYwfzEjMCEGCSqGSIb3DQEJARYUc3VwcG9ydEBjcnlwdG9wcm8
ucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxFzAVBgNVBAoTDkNSWVBUTy1QUk8gTExDMSEw
HwYDVQQDExhDUllQVE8tUFJPIFRlc3QgQ2VudGVyIDICExIAMDQ7LGEnh5qkeuoAAAAwNDswCgYGKoUDA
gIJBQCgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0xOTAzMjExNDA3NT
VaMC8GCSqGSIb3DQEJBDEiBCAe11xSW84uFGqdtPvBGhfcnLulI56pFmp7uUxqhAxpejAKBgYqhQMCAhM
FAARAdb2bikqzGQ7PGAPQMq8P7dpHUL57SNzW8uaym2OjrdZ8u17EP/NnQZANHLSI64TMd+LbTFTCMzpI
/48jmvlFLA==</ns2:SignaturePKCS7></ns2:RefAttachmentHeader></ns2:RefAttachmentHea
derList>
<BusinessProcessMetadata/>
</SenderProvidedRequestData>

<CallerInformationSystemSignature><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:Canonicalization
Method 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_CALLER"><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>inQsriiui8V1gYG/eQV1GJkWjS6NXm5HH5xymMdBDq4=</ds
:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>I6GILCzT+x19g35sy0
o0D6F4D3cgjkJdZybVSuw265KY7lHTfetl642SPhgDhFgFROfhxS8PNNHd
Gdk97eaJ1w==</ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIID
LDCCAtugAwIBAgITEgAwNDssYSeHmqR66gAAADA0OzAIBgYqhQMCAgMwfzEjMCEGCSqGSIb3
DQEJARYUc3VwcG9ydEBjcnlwdG9wcm8ucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cx
FzAVBgNVBAoTDkNSWVBUTy1QUk8gTExDMSEwHwYDVQQDExhDUllQVE8tUFJPIFRlc3QgQ2VudGVy
IDIwHhcNMTgxMjEyMTMyNTA5WhcNMTkwMzEyMTMzNTA5WjA+MRAwDgYDVQQDDAdteV90ZXN0MQ8w
DQYDVQQKDAZSVExhYnMxGTAXBgkqhkiG9w0BCQEWCnRlc3RAdHMucnUwYzAcBgYqhQMCAhMwEgYH
KoUDAgIjAQYHKoUDAgIeAQNDAARALSydgtZTKw9ECi+2FUqL90Yn5y+hKuGkCDjGwar2AzbdWUOm
8WIjEFEtQHjON7wHS1w8koXvxHJ9jr6zFvCN2qOCAW0wggFpMBMGA1UdJQQMMAoGCCsGAQUFBwME
MAsGA1UdDwQEAwIGwDAdBgNVHQ4EFgQUZ7oyl4Vjj4M3FQ+P29yp7Lf4h10wHwYDVR0jBBgwFoAU
FTF8sI0a3mbXFZxJUpcXJLkBeoMwWQYDVR0fBFIwUDBOoEygSoZIaHR0cDovL3Rlc3RjYS5jcnlw
dG9wcm8ucnUvQ2VydEVucm9sbC9DUllQVE8tUFJPJTIwVGVzdCUyMENlbnRlciUyMDIuY3JsMIGp
BggrBgEFBQcBAQSBnDCBmTBhBggrBgEFBQcwAoZVaHR0cDovL3Rlc3RjYS5jcnlwdG9wcm8ucnUv
Q2VydEVucm9sbC90ZXN0LWNhLTIwMTRfQ1JZUFRPLVBSTyUyMFRlc3QlMjBDZW50ZXIlMjAyLmNy
dDA0BggrBgEFBQcwAYYoaHR0cDovL3Rlc3RjYS5jcnlwdG9wcm8ucnUvb2NzcC9vY3NwLnNyZjAI
BgYqhQMCAgMDQQAoeTnuXVpWLiCG052JlgkFsmD9g/nxgoPpTmj4W1YrS7b6I+0f4RM/IuJbcD7+
vM25L5mxNBc8ozvEh5PkP83l</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Sign
ature></CallerInformationSystemSignature></SendRequestRequest>

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 (ДБО КО или ИС КО) по токену доступа
400	ADR-0100	Недопустимый вид сведений
400	ADR-0101	Неверные идентификаторы вложений. Идентификаторы вложений не соответствуют XML запроса

Код ответа HTTP	Значение параметра «code»	Описание ошибки
400	ADR-0102	Представлена невалидная XML
400	ADR-0104	Передан неверный тип XML на подпись (разрешенный тип сообщения для СМЭВ)

3.8.2. Функция «Проверить подпись»

Функция принимает на вход:

- СМЭВ-конверт с ответом, который ИС КО получает из СМЭВ;
- СМЭВ-конверт с ответом о статусе ранее отправленного в СМЭВ сообщения, которое ИС КО 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 4.2;
- 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 СОС 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
```

Заголовки запроса:

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

Где,

{{token}} - токен доступа ИС КО к API.

Входные параметры в теле запроса в формате JSON:

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:Mess
ageMetadata><ns2:SMEVSignature><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:Canonicalization
Method 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
:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>ZTkM8zPI9ght+tkarw
```

```
9jDUyzm4Xwo1jwErVBH0BfZ24YBBNk3zJxERtbZJkjLvh3As7mE+B7E8n6dB2SRLWOQA==</ds:Signat
ureValue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIIH2DCCB4egAwIBAgIRAXILAVZ
QABCz6RGAPpV5agEwCAYGKoUDAgIDMIIBRjEYMBYGBSqFA2QBEg0xMjM0NTY3ODkwMTIzMRowGAYIKoUD
A4EDAQESDDAwMTIzNDU2Nzg5MDEpMCcGA1UECQwg0KHRg9GJ0LXQstGB0LrQuNC5INCy0LDQuyDQtC4gM
jYxFzAVBgkqhkiG9w0BCQEWCGNhQHJ0LnJ1MQswCQYDVQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB0L
rQstCwMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoMG9Ce0JDQniDQoNC+0YHRgtC10LvQtdC
60L7QvDEwMC4GA1UECwwn0KPQtNC+0YHRgtC+0LLQtdGA0Y/RjtGJ0LjQuSDRhtC10L3RgtGAMTQwMgYD
VQQDDCvQotC10YHRgtC+0LLRi9C5INCj0KYg0KDQotCaICjQoNCi0JvQsNCx0YEpMB4XDTE5MDMwNDEzM
Dg0MFoXDTIwMDMwNDEzMTg0MFowggELMR8wHQYJKoZIhvcNAQkCDBDQotCh0JzQrdCSM1/QmtCaMRowGA
YIKoUDA4EDAQESDDAwNzcwNzA0OTM4ODEYMBYGBSqFA2QBEg0xMDI3NzAwMTk4NzY3MSgwJgYDVQQKDB/
Qn9CQ0J4gwqvQoNC+0YHRgtC10LvQtdC60L7QvMK7MSYwJAYDVQQHDB3QodCw0L3QutGCLdCf0LXRgtC1
0YDQsdGD0YDQszEpMCcGA1UECAwgNzgg0KHQsNC90LrRgi3Qn9C10YLQtdGA0LHRg9GA0LMxCzAJBgNVB
AYTAlJVMSgwJgYDVQQDDB/Qn9CQ0J4gwqvQoNC+0YHRgtC10LvQtdC60L7QvMK7MGMwHAYGKoUDAgITMB
IGByqFAwICJAAGByqFAwICHgEDQwAEQN9eHf5trruzGfhJPjeX9nlXFGtOI+U36xVVsGczNTz8kwwgnt6
h0yGTkT296O9cmb/4ZnaUSbj4vvIMQAzXejajggSDMIIEfzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYE
FPnxGNuqnYf86yewtnZ3KsHOW0GZMIIBiAYDVR0jBIIBfzCCAXuAFD7vGT8PuXmw8eYpIaPkuZW5pe6Qo
YIBTqSCAUowggFGMRgwFgYFKoUDZAESDTEyMzQ1Njc4OTAxMjMxGjAYBggqhQMDgQMBARIMMDAxMjM0NT
Y3ODkwMSkwJwYDVQQJDCDQodGD0YnQtdCy0YHQutC40Lkg0LLQsNC7INC0LiAyNjEXMBUGCSqGSIb3DQE
JARYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRgwFgYDVQQIDA83NyDQnNC+0YHQutCy0LAxFTATBgNVBAcM
DNCc0L7RgdC60LLQsDEkMCIGA1UECgwb0J7QkNCeINCg0L7RgdGC0LXQu9C10LrvtC8MTAwLgYDVQQLD
CfQo9C00L7RgdGC0L7QstC10YDRj9GO0YnQuNC5INGG0LXQvdGC0YAxNDAyBgNVBAMMK9Ci0LXRgdGC0L
7QstGL0Lkg0KPQpiDQoNCi0JogKNCg0KLQm9Cw0LHRgSmCEQFyCwFWUAC5s+cRzzq+NHegMB0GA1UdJQQ
WMBQGCCsGAQUFBwMCBggrBgEFBQcDBDAnBgkrBgEEAYI3FQoEGjAYMAoGCCsGAQUFBwMCMAoGCCsGAQUF
BwMEMB0GA1UdIAQWMBQwCAYGKoUDZHEBMAgGBiqFA2RxAjArBgNVHRAEJDAigA8yMDE5MDMwNDEzMDg0M
FqBDzIwMjAwMzA0MTMwODQwWjCCATQGBSqFA2RwBIIBKTCCASUMKyLQmtGA0LjQv9GC0L7Qn9GA0L4gQ1
NQIiAo0LLQtdGA0YHQuNGPIDMuOSkMLCLQmtGA0LjQv9GC0L7Qn9GA0L4g0KPQpiIgKNCy0LXRgNGB0Lj
QuCAyLjApDGPQodC10YDRgtC40YTQuNC60LDRgiDRgdC+0L7RgtGB0YLQstC40Y8g0KTQodCR
INCg0L7RgdGB0LjQuCDihJYg0KHQpC8xMjQtMjUzOSDQvtGCIDE1LjAxLjIwMTUMY9Ch0LXRgNGC0LjRh
NC40LrQsNGCINGB0L7QvtdGC0LLQtdGC0YHRgtCy0LjRjyDQpNCh0JEg0KDQvtGB0YHQuC4IOKEliDQod
CkLzEyOC0yODgxINC+0YIgMTIuMDQuMjAxNjA2BgUqhQNkbwQtDCsi0JrRgNC40L/RgtC+0J/RgNC4IEN
TUCIgKNCy0LXRgNGB0LjRjyAzLjkpMGUGA1UdHwReMFwwWqBYoFaGVGh0dHA6Ly9jZXJ0ZW5yb2xsLnRl
c3QuZ29zdXNsdWdpLnJ1L2NkcC8zZWVmMTkzZjBmYjk3OWIwZjFlNjI5MjFhM2U0Yjk5NWI5YTVlZTkwL
mNybDBXBggrBgEFBQcBAQRLMEkwRwYIKwYBBQUHMAKGO2h0dHA6Ly9jZXJ0ZW5yb2xsLnRlc3QuZ29zdX
NsdWdpLnJ1L2NkcC90ZXN0X2NhX3J0bGFiczIuY2VyMAgGBiqFAwICAwNBACD706a8WMDdiFimYlNM7J6
VNBgz4EoqSGhxWpn1iCIJysDDjGih66xC2PvWq7Cjz2uqWAIcFPEo6mMF6cINJ/8=</ds:X509Certifi
cate></ds:X509Data></ds:KeyInfo></ds:Signature></ns2:SMEVSignature></ns2:SendRequ
estResponse>
```


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 (ДБО КО или ИС КО) по токену доступа
400	ADR-0102	Представлена невалидная XML
400	ADR-0103	Передан неверный тип XML на проверку подписи (разрешенный тип сообщения для СМЭВ)

3.9.Функции "Проверки состояния модулей Адаптера"

Данная функция рекомендуется к использованию системой мониторинга КО для контроля функционирования модулей Адаптера. Вызовы осуществляются в пределах контролируемой зоны КО. 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 ДБО КО.

Поддерживаемый метод HTTP запроса:

```
GET
```

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

```
/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 КО к API.

Пример запроса:

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

Функция возвращает ответ с HTTP-кодом, сигнализирующем 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.

4. Криптографические алгоритмы

4.1.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 Р 34.10-2001;
- вычисление значения хэш-функции в соответствии с алгоритмами ГОСТ Р 34.11-2012 (256/512 бит) и ГОСТ Р 34.11-94.

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.

4.2.Требования к проверке ЭП в Адаптере

При проверке ЭП Адаптер проводит проверки действительности сертификатов:

- проверка ЭП сертификатов из цепочки сертификатов КО и сертификатов ГУЦ;
- проверка сроков действия сертификатов из цепочки сертификатов КО и сертификатов ГУЦ;
- проверка области использования сертификата КО 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.

ПРИЛОЖЕНИЕ Е. Руководство администратора по типовому решению информационной безопасности

1. Общие сведения

1.1.Полное наименование и условное обозначение Системы

Полное наименование и условное обозначение системы: Программно-аппаратный комплекс электронной подписи биометрических данных при подключении к Единой биометрической системе.

Условное обозначение: Адаптер, Система.

1.2.Перечень реализуемых функций

Для решения задач, подлежащих автоматизации, Адаптер выполняет следующие группы (комплексы) функций:

- группа функций процесса удаленной идентификации для решения задачи работы в рамках протокола OpenId Connect со стороны клиента (банка, проводящего авторизацию пользователя с использованием его биометрических данных - удаленную идентификацию) (внутренний API верификации Адаптера);
- группа функций процесса удаленной идентификации для решения задачи работы в рамках протокола OpenId Connect со стороны пользователя (внешний API верификации Адаптера);
- группа функций получения результата верификации для ДБО КО (API получения результата верификации ДБО КО);
- 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 управления, журналирования и мониторинга.

Группа функций управления, журналирования и мониторинга является вспомогательной и обеспечивает управление компонентами Адаптера и контроль их работоспособности.

1.3.Сведения о техническом и программном обеспечении Адаптера

Серверное программное обеспечение:

1. Операционная система Astra Linux SE 1.6.
1. ГосJava 1.8.x.
2. Сервер БД PostgreSQL не ниже 9.5.
3. Контейнер сервлетов Apache Tomcat не ниже 8.5.
4. СКЗИ «КриптоПро CSP» версия 4.0.
5. Модуль «КриптоПро JavaCSP».

Для модуля «КриптоПро JavaCSP» также нужно установить дополнительные пакеты:

1. CADES.
2. cpkix-jdk15on-1.50.jar и bcprov-jdk15on-1.50.jar.

3. xmlsec-1.5.0.jar, commons-logging-1.1.1.jar и xalan-2.7.0.jar.

Требуемое программное обеспечение можно скачать из репозитория http://packages.lab50.net/.

Для эксплуатации Системы требуются следующие виды технических средств:

- серверное оборудование с характеристиками не ниже:
- процессоры 2.6 ГГц;
- от 8 физических ядер;
- архитектура x86-64;
- хранение данных от 50 Gb (2 HDD, RAID 10);
- оперативное хранение от 64 Gb RAM с ECC;
- сетевая плата Ethernet 2*GE;
- сетевая плата Ethernet с двумя оптическим выходами SC;
- разъемы: от 1 PCIe;
- 2 блока питания (резервирование);
- TLS-шлюзы класса КС3 с поддержкой отечественных и зарубежных алгоритмов;
- в качестве HSM класса КВ2 используется ПАКМ «КриптоПро HSM» версия 2.0;
- межсетевые экраны 3 класса, по требованиям ФСТЭК;
- средство обнаружения вторжений 3 класса уровня сети по требованиям ФСТЭК;
- средства антивирусной защиты класса 2 тип Б по требованиям ФСТЭК;
- аппаратно программный модуль доверенной загрузки "Соболь" (версий 3.0, 3.1 или 3.2).

2. Структура Адаптера

Структурная схема Адаптера представлена на рисунке ниже (Рисунок 12).

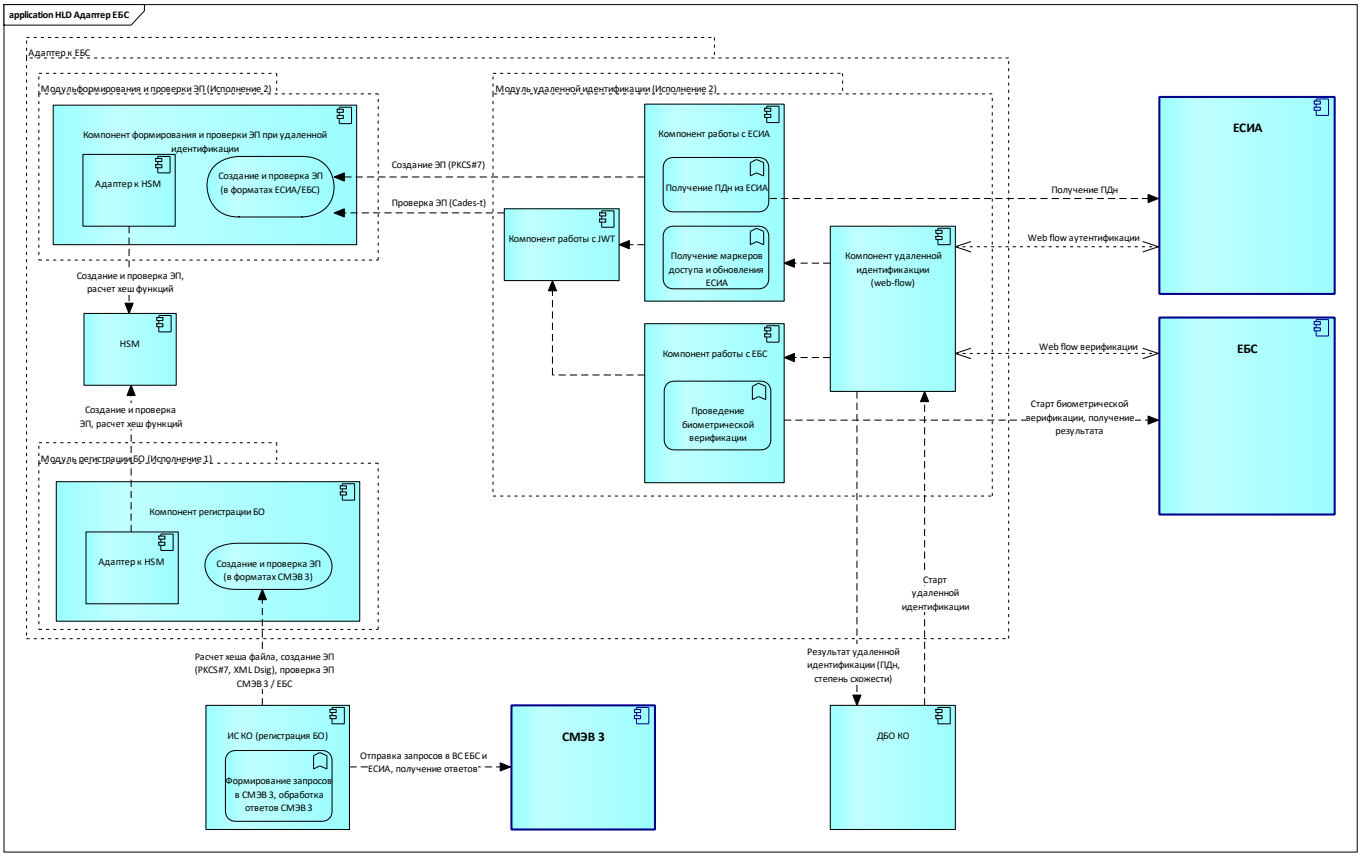

Рисунок 12

Адаптер состоит из следующих функциональных модулей (см. Таблица **5**)

Таблица 5. Перечень функциональных модулей Адаптера ЕБС

№	Наименование модуля	Исполнение	Функции модуля
1	Модуль регистрации БО	Исполнение 1	Взаимодействие со СМЭВ 3 в рамках процесса размещения или обновления в ЕБС биометрических персональных данных (создание и проверка ЭП)
2	Модуль формирования и проверки ЭП	Исполнение 2	Взаимодействие с ЕСИА и ЕБС в рамках протокола OpenId Connect для идентификации, аутентификации и авторизации пользователя с использованием его биометрической информации (создание и проверка ЭП)
3	Модуль удаленной идентификации		

Адаптер разработан в двух исполнениях.

Исполнение 1, предназначенное для:

– взаимодействия со СМЭВ 3 в рамках процесса размещения или обновления в ЕБС биометрических персональных данных (создание и проверка ЭП).

Исполнение 2, предназначенное для:

– взаимодействия со СМЭВ 3 в рамках процесса размещения или обновления в ЕБС биометрических персональных данных (создание и проверка ЭП);

– взаимодействия с ЕСИА и ЕБС в рамках протокола OpenId Connect для идентификации, аутентификации и авторизации пользователя с использованием его

биометрической информации (создание и проверка ЭП).

Сетевая схема взаимодействия технических средства защиты каналов взаимодействия приведена на рисунке ниже (Рисунок 13).

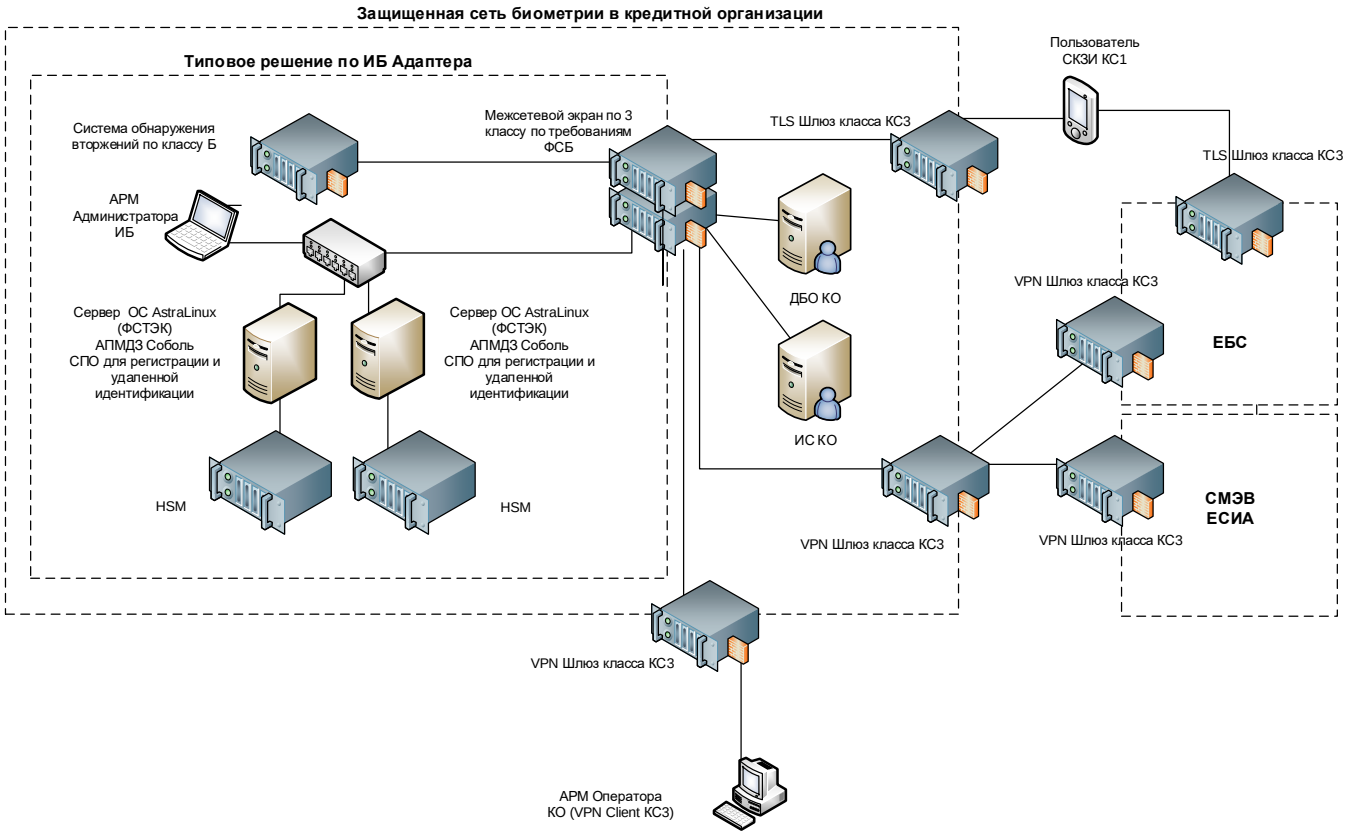

Рисунок 13

Требований к способам связи при сетевом информационном обмене между компонентами Системы в пределах контролируемой зоны Адаптера не предъявляется.

В случае передачи информации между компонентами Системы в открытом виде необходимо обеспечивать защиту от внутреннего нарушителя путем размещения данных компонент в рамках одной опечатываемой серверной стойки, находящейся в рамках контролируемой зоны.

Структурная схема взаимодействия Адаптера и смежных систем в контексте процессов удаленной идентификации и регистрации БО с указанием требований к защите каналов взаимодействия приведена на рисунке ниже (см. Рисунок 14).

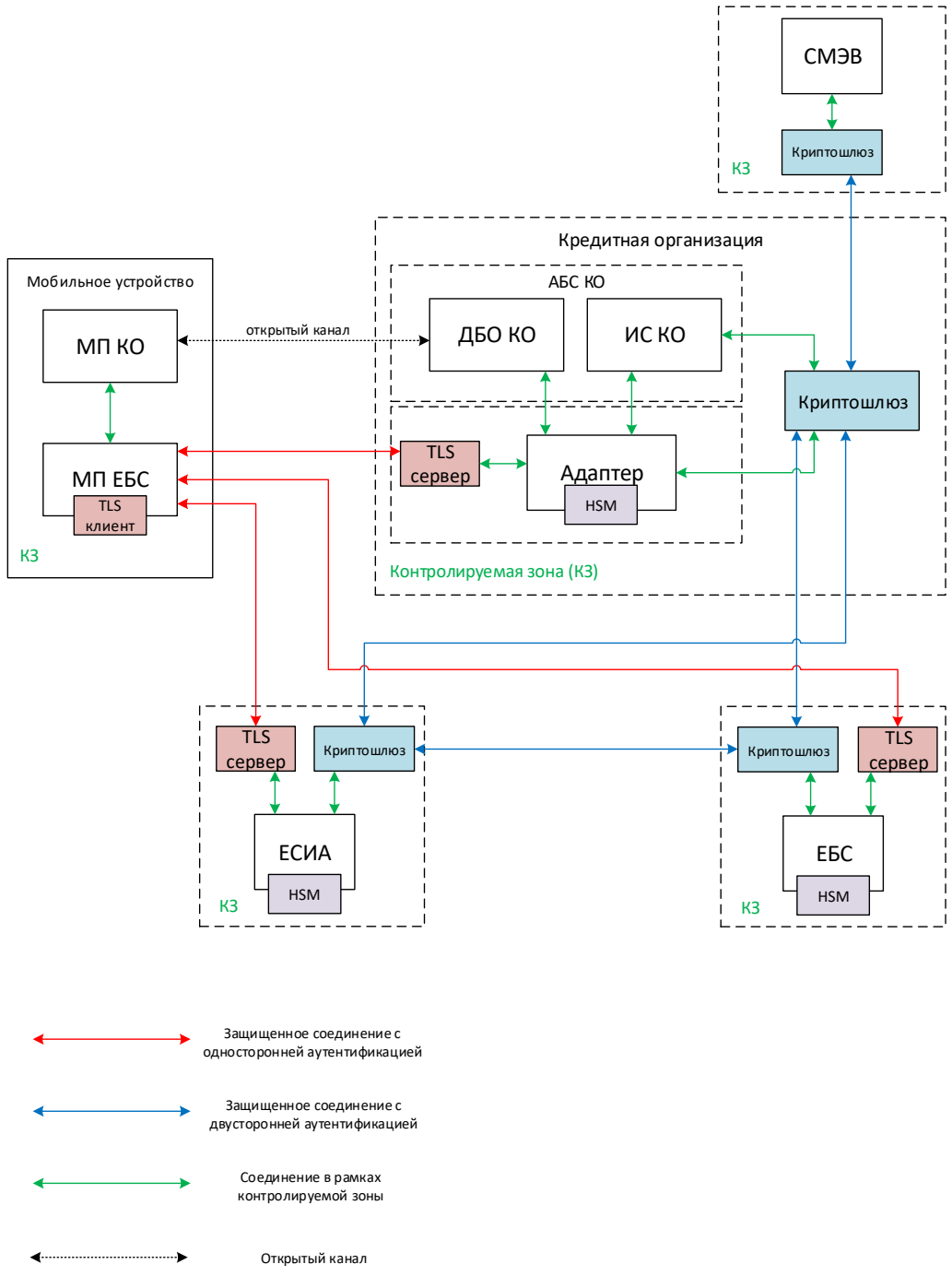

Рисунок 14

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

– между ИС КО 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:

– применяются СКЗИ на устройстве пользователя, сертифицированные по классу КС1;

– применяются СКЗИ на стороне Адаптера, сертифицированные по классу КС3.

Соединение в рамках контролируемой зоны - мобильного устройства пользователя осуществляется с использованием средств взаимодействия между мобильными приложениями операционной системы мобильного устройства. Прикладной программный интерфейс данного взаимодействия реализуется согласно Методическим рекомендациям по работе с ЕБС.

Канал связи между устройством пользователя (мобильным приложением ЕБС) и Адаптером защищен с использованием протокола TLS с односторонней аутентификацией (аутентификация TLS-шлюза на стороне Адаптера). Реализация протокола TLS в TLS-шлюзе 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)".

В рамках протокола удаленной идентификации по открытому каналу между мобильным приложением банка и ДБО КО передаются:

- запрос от пользователя к ДБО КО на предоставление услуги, требующий аутентификации;
- ответ от ДБО КО, содержащий перенаправление на Адаптер для прохождения удаленной аутентификации с указанием сгенерированного ДБО КО идентификатора 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.

Для СКЗИ ПАКМ «КриптоПро HSM» версия 2.0, входящих в состав Адаптера, при их размещении и настройке следует руководствоваться согласованной с ФСБ России документацией на каждое СКЗИ в части требуемых мер по обеспечению целостности среды функционирования СКЗИ.

Для ОС "Astra Linux Special Edition" при ее установке и настройке на серверах КТС Системы следует руководствоваться документацией на ОС в части требуемых мер по обеспечению контроля целостности.

2.1.Роли в системе разграничения доступа

В функционировании системы 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 системы;
- 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 Системы;
- 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 системы;
- управление правами доступа пользователей к функциям системы;
- 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 системы во всех режимах функционирования.

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

Запрещается вносить изменения в состав, конструкцию, электрическую и монтажную схему HSM.

3. Настройка Адаптера

3.1.Состав и содержание дистрибутивного носителя данных

Дистрибутив специального программного обеспечения программно-аппаратного комплекса электронной подписи биометрических данных поставляется в виде deb пакетов:

1. adapter.deb - сервис удаленной идентификации;
2. crypto-server-engine.deb - сервис подписания;
3. inner-smev-service.deb - сервис регистрации.

3.2.Установка дистрибутива

1. Установка дистрибутива производится с помощью пакетного менеджера dpkg, для этого необходимо выполнить следующие команды:

```
dpkg -i adapter.deb
dpkg -i crypto-server-engine.deb
dpkg -i inner-smev-service.deb
```

2. В ходе установки в диалоговом интерфейсе пользователю необходимо будет ввести значения параметров, которые затем будут сохранены в сгенерированные файлы конфигураций адаптера.
3. Отредактировать конфигурационный файл /etc/tomcat8/catalina.properties, добавив строки, содержащие пути до конфигурационных файлов адаптера:

```
configFileName=«/etc/adapter/adapter_properties.json»
confVrfPath=«/etc/crypto-server-engine/application.properties»
confRegPath=«/etc/inner-smev-service/application.properties»
```

3.2.1. Описание параметров пакета adapter.deb

Конфигурационные параметры пакета хранятся в файле «/etc/adapter/adapter_properties.json» и разделены на блоки:

1. "database_connection"
   - tableName - Имя таблицы в базе данных;
   - dataSourceClassName - Имя класса БД, предоставляемого драйвером JDBC;
   - maximumPoolSize - Максимальное количество подключений к базе данных;
   - maxLifetime - Максимальное время жизни соединения в пуле (в миллисекундах);
   - idleTimeout - Максимальное время, в течение которого соединение может находиться в пуле в режиме ожидания (в миллисекундах);
   - serverName - Имя сервера для jdbc подключения к базе данных;
   - portNumber - Порт для jdbc подключения к базе данных;
   - databaseName - Название базы данных для jdbc подключения;
   - user - Пользователь базы данных;
   - password - Пароль пользователя базы данных;
   - cachePrepStmts - Использовать подготовленные запросы к базе данных;
   - prepStmtCacheSize - Количество подготовленных запросов, которые будут кэшироваться для каждого соединения;
   - prepStmtCacheSqlLimit - Максимальная длина подготовленного запроса, который будет кешироваться;

- sessionLifetime - Время жизни сессии пользователя (в миллисекундах)

2. "servlets_config"
   - bearer - Авторизационный токен;
   - external_sid_size - Ограничение на длину session id (sid), который присылает банк при создании сессии
3. "pki_client_config"
   - servers_url - Список серверов PKI через запятую;
   - sign_urn - Urn для указания сервиса PKI для подписания;
   - verify_urn - Urn для указания сервиса PKI для проверки подписи;
   - check_urn - Urn для указания сервиса PKI для проверки состояния сервиса;
   - amount_retry - Количество попыток переподключения к PKI серверам;
   - timeout_retry - Таймаут между переподключениями к PKI серверам (в милисекундах);
   - timeout_healthcheck - Таймаут между проверками PKI серверов (в милисекундах)
4. "dbo_client_config"
   - result_url — Url для перенаправления пользователя в случае возникновения ошибки
5. "ebs_client_config"
   - redirect_uri - Название параметра, в котором передаются redirect ссылки для возврата в адаптер;
   - start_url - Ссылка на эндпойнт ЕБС для прохождения верификации;
   - get_verify_url_format - Ссылка-шаблон на endpoint получения результата верификации
6. "esia_client_config"
   - esia_ac_url - Ссылка на endpoint ЕСИА для аутентификации пользователя;
   - esia_te_url - Ссылка на endpoint ЕСИА для получения токена на запрос результатов верификации;
   - esia_prns_url - Ссылка на endpoint ЕСИА для получения персональных данных пользователя
7. "processing_config"
   - create_new_state_for_esia - Создать новое состояние для ЕСИА;
   - client_id - Мнемоника информационной системы в ЕСИА;
   - pki_auth_verify_ebs - Авторизационный токен PKI для проверки подписи JWT, полученной от ЕБС;
   - pki_auth_sign_esia - Авторизационный токен PKI для подписания client_secret ЕСИА;

- pki_auth_health_check - Авторизационный токен для проведения healthcheck PKI

8. "redirect_uri_config"
   - redirect_uri_verification_servlet - Ссылка на endpoint адаптера для прохождения верификации;
   - redirect_uri_result_servlet - Ссылка на endpoint адаптера для обращения за токеном верификации (поход в esia_te_url);
   - redirect_uri_end_servlet - Ссылка на endpoint адаптера для получения персональных данных

3.2.2. Описание параметров пакета crypto-server-engine.deb

Конфигурационные параметры пакета хранятся в файле «/etc/crypto-server-engine/application.properties»:

- containerType - идентификатор хранилища ключевых пар (например, для КриптоПРО - HDIMAGE в случае локального хранилища, HSMDB - в случае использования HSM);
- keyFilepath - полный путь до локального файла с информацией по ключам для подписи и сертификатам;
- bearerFilePath - полный путь до файла с настройками информацией о пользователях (см. п. про Настройка пользователей);
- jksFilePath - полный путь до локального JKS-файла - хранилище сертификатов, необходимых для проверки сертификата;
- jksPassword - пароль от JKS-файла, указанного в параметре jksFilePath;
- tsa.hostname - адрес сервера штампа времени для CADES-T;
- healthcheck.keyId - идентификатор ключа для выполнения функции проверки работоспособности.

3.2.3. Описание параметров пакета inner-smev-service.deb

Конфигурационные параметры пакета хранятся в файле «/etc/inner-smev-service/application.properties»:

- containerType - идентификатор хранилища ключевых пар (например, для КриптоПРО - HDIMAGE в случае локального хранилища, HSMDB - в случае использования HSM);
- keyFilepath - полный путь до локального файла с информацией по ключам для подписи и сертификатам;
- bearerFilePath - полный путь до файла с настройками информацией о пользователях
- jksFilePath - полный путь до локального JKS-файла - хранилище сертификатов, необходимых для проверки сертификата;
- jksPassword - пароль от JKS-файла, указанного в параметре jksFilePath;

- namespaces (опционально) - полный путь до файла с настройками пространств имен XML, используемых при общении со СМЭВ;
- healthcheck.keyId - идентификатор ключа для выполнения функции проверки работоспособности.

3.2.4. Завершение установки

После установки скопировать файл log4j-1.2.17 из /var/lib/tomcat8/webapps/servlets/WEB-INF/lib/ в директорию /var/lib/tomcat8/lib/.

Дополнительно можно настроить отправку сообщений по протоколу SYSLOG в файлах:

- /var/lib/tomcat8/webapps/servlets/WEB-INF/classes/log4j.properties;
- /var/lib/tomcat8/webapps/crypto-server-engine/WEB-INF/classes/log4j.properties;
- /var/lib/tomcat8/webapps/inner-smev-service/WEB-INF/classes/log4j.properties

Настраиваемые параметры:

- log4j.appender.SYSLOG.syslogHost - хост сервера syslog;
- log4j.appender.SYSLOG.facility - syslog facility.

3.3.Настройка программного обеспечения сервера PostgreSQL

1. Создать роль в Postgresql:

```
CREATE ROLE adapter WITH createdb login password 'adapter';
```

2. Создать базу данных в Postgresql:

```
CREATE DATABASE adapter OWNER adapter;
```

3. Создать таблицу и индекс:

```
CREATE TABLE IF NOT EXISTS adapter (
external_sid VARCHAR(50) NOT NULL,
internal_sid VARCHAR(50),
session_data json,
state VARCHAR(50) NOT NULL,
session_time BIGINT NOT NULL,
PRIMARY KEY (external_sid)
);
CREATE UNIQUE INDEX idx_internal_sid
ON adapter (internal_sid);
```

4. В конфигурационном файле pg_hba.conf добавить запись:

```
host  all   adapter,adapter 0.0.0.0/0 md5
```

4. Проверка работоспособности

4.1.Методы проверки

Методы возвращают текущее состояние работоспособности модуля, обеспечивающего процесс регистрации БО и модуля, обеспечивающего процесс удаленной идентификации.

Входные параметры: отсутствуют.

Выходные параметры: отсутствуют.

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.

Пример запроса:

1. Для проверки состояния модуля, обеспечивающего процесс регистрации БО (относительно базового URL):

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

2. Для проверки состояния модуля, обеспечивающего процесс удаленной идентификации (относительно базового URL):

```
GET /api/v1/vrf/check HTTP/1.1
```

Пример ответа:

1. Для проверки состояния модуля, обеспечивающего процесс регистрации БО (относительно базового URL):

```
HTTP/1.1 200 OK
```

2. Для проверки состояния модуля, обеспечивающего процесс удаленной идентификации (относительно базового URL):

```
HTTP/1.1 200 OK
```

4.2.Аварийные ситуации

В случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств для восстановления штатного функционирования оборудования Адаптера необходимо произвести перезагрузку общесистемного ПО.

При ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функции Подсистемы возлагается на ОС.

При ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на ОС. Действия в случаях обнаружения несанкционированного вмешательства в данные.

Действия в случае обнаружения несанкционированного вмешательства в данные определяются политикой информационной безопасности организации.

При неверных действиях пользователей, неверных форматах или недопустимых значениях входных данных, система выдаёт пользователю соответствующие сообщения.

5. Подготовка объекта автоматизации

5.1.Условия функционирования объекта автоматизации

КО необходимо создание следующих условий функционирования объекта автоматизации:

- обеспечить подключение к ЕСИА, согласно регламентам и инструкциям для подключения к ЕСИА;
- обеспечить подключение к СМЭВ 3, согласно регламентам и инструкциям для подключения к СМЭВ 3.x;
- произвести пуско-наладочные работы КТС Адаптера в инфраструктуре КО, с учетом рекомендаций раздела 5.2;
- настроить Адаптер согласно руководству администратора;
- обеспечить сетевые доступы для взаимодействий Адаптера со смежными Системами и пользователями;
- обеспечить сетевые доступы от Адаптера до СОС и OCSP-служб, аккредитованных УЦ для проверки актуальности сертификатов ЭП;
- настроить СЗИ КО:
- средства межсетевого экранирования уровня приложений (WAF);
- средства защиты от отказа в обслуживании (DDOS);
- средства предотвращения вторжений (IPS);
- создать подразделения и службы, необходимые для функционирования Системы.

5.2.Дополнительные требования к размещению оборудования

При размещении технических средств Адаптера следует руководствоваться технической документацией на данные технические средства. Для СКЗИ ПАКМ «КриптоПро HSM» версия 2.0, входящих в состав Адаптера, при их размещении следует руководствоваться согласованной с ФСБ России документацией на каждое СКЗИ.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства серверов, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях.

Входные двери режимных помещений должны быть оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время.

Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

По окончании рабочего дня помещения закрываются и опечатываются. Помещения с опечатанными входными дверьми сдаются под охрану отделу безопасности или дежурному по предприятию (по установленному порядку) с указанием времени приема-сдачи с отметкой о включении и выключении охранной сигнализации в журнале учета.

Сдачу ключей и помещений под охрану, также получение ключей и вскрытие помещений производят сотрудники, работающие в этих помещениях, по утвержденному руководством учреждения списку, который находится у охраны или у дежурного по учреждению.

В случае утраты ключа от входной двери помещения немедленно ставится в известность отдел безопасности учреждения.

На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.