

Сервис удаленной идентификации ГИС ЕБС (mWeb-to-App)

1.1. Требования для подключения сервиса удаленной идентификации ГИС ЕБС

ИС, участвующие в процессе удаленной идентификации:

- ИС МФО (Потребителя БДн);
- Web-версия мобильного приложения МФО;
- Адаптер;
- ЕСИА;
- ГИС ЕБС.

Предварительные условия:

- использование физическим лицом (ФЛ) web-версии МП МФО (Потребителя БДн);
- использование ФЛ сервиса МП «Госуслуги Биометрия»;
- согласие ФЛ на предоставление БДн;
- ФЛ имеет подтвержденную УЗ ЕСИА;
- МФО зарегистрирована в ГИС ЕБС в роли Потребителя БДн;
- МФО зарегистрирована в ЕСИА;
- наличие камеры и микрофона на устройстве ФЛ.

Для подключения к сервису удаленной идентификации ГИС ЕБС МФО необходимо:

1. Зарегистрировать ИС в продуктивном контуре ЕСИА в соответствии с регламентом информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства (последняя версия опубликована по адресу: <https://digital.gov.ru/documents/reglament>) и Методическими рекомендациями по использованию ЕСИА (последняя версия опубликована по адресу: <https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia>).

2. Подать заявку на регистрацию ИС и получение доступа к сервисам аутентификации в тестовом контуре ЕСИА в соответствии с регламентом информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства

(последняя версия опубликована по адресу: <https://digital.gov.ru/documents/reglament>) и Методическими рекомендациями по использованию ЕСИА (последняя версия опубликована по адресу: <https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia>).

3. Подать заявку на регистрацию ИС в тестовой среде ГИС ЕБС в роли Потребителя БДн в соответствии с п. 9.1.3 Регламент взаимодействия с ГИС ЕБС (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Технические документы») и Методическими рекомендациями по работе с ГИС ЕБС для разработчиков (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Методические рекомендации, инструкции, памятки»).

4. Произвести акцепт оферты о «заключении соглашения об оказании услуг по предоставлению информации о степени соответствия предоставленных клиентом - физическим лицом биометрических персональных данных векторам единой биометрической системы, содержащимся в Единой биометрической системе», опубликованной по адресу в разделе «Тарифы, оферты, соглашения» и в ЛК ЮЛ в разделе «Оферты».

5. Организовать защищенный канал в соответствии с разделом 12.1.1 Регламента информационного взаимодействия участников биометрических процессов с ГИС ЕБС (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Технические документы»).

6. Подать заявку на получение доступа к сервисам аутентификации в продуктивном контуре ЕСИА в соответствии с регламентом информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства (последняя версия опубликована по адресу: <https://digital.gov.ru/documents/reglament>) и Методическими рекомендациями по использованию ЕСИА (последняя версия опубликована по адресу: <https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia>).

7. Подать заявку на подключение ИС к продуктивной среде ГИС ЕБС в роли Потребителя БДн в соответствии с п. 9.2.3 Регламента информационного взаимодействия участников биометрических процессов с ГИС ЕБС и Методическими рекомендациями по работе с

ГИС ЕБС для разработчиков (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Технические документы») и Методическими рекомендациями по работе с ГИС ЕБС для разработчиков (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Методические рекомендации, инструкции, памятки»).

Подробное описание требований для подключения к сервису удаленной идентификации в ГИС ЕБС содержится в п. 7.2, 9.1.3, 9.2.3, 12.1.1, 10.3 Регламента информационного взаимодействия участников биометрических процессов с ГИС ЕБС (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Технические документы»), а также в пошаговой инструкции, размещенной в ЛК ЮЛ на сайте и в Демо ЛК (<https://ebs.ru/documents/>).

1.2. Требования к настройке ИС МФО – Потребителя БДн

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

- Осуществить реализацию взаимодействия ИС МФО и ЕСИА в соответствии с разделом 3 Методических рекомендаций по использованию ЕСИА (последняя версия опубликована по адресу: <https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia>).
- Осуществить настройку доступа к сервису авторизации продуктивной ЕСИА (Точка доступа к ЕСИА) в соответствии с Приложением Б к Методическим рекомендациям по работе с ГИС ЕБС для разработчиков (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Методические рекомендации, инструкции, памятки»).
- Осуществить настройку получения маркера доступа и авторизационного кода в соответствии с разделом 5.2.1 Методических рекомендаций по работе с ГИС ЕБС для разработчиков (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Методические рекомендации, инструкции, памятки») и приложением В.2 Методических рекомендаций по использованию ЕСИА (последняя версия опубликована по адресу: <https://ebs.ru/documents/>).
- Осуществить реализацию взаимодействия ИС МФО с ТИБ в соответствии с документацией, опубликованной по адресу: <https://ebs.ru/documents/tibkriptosdktls/>

1.3. Процедура прохождения удаленной идентификации при помощи глубинной ссылки (deeplink) с переходом из мобильной web-версии приложения МФО в МП «Госуслуги Биометрия»

Алгоритм процесса прохождения процедуры удаленной идентификации mWeb-to-App:

1. Пользователь инициирует процесс получения услуги в мобильной web-версии приложения МФО.
2. Web-версия МП МФО выполняет запрос в ИС МФО для старта процесса удаленной идентификации.
3. ИС МФО генерирует уникальный идентификатор (sid) и отправляет запрос на создание сессии верификации в Адаптер (см. Приложение В, раздел 3.4.1 Методические рекомендации по работе с ГИС ЕБС для разработчиков (последняя версия опубликована по адресу: <https://ebs.ru/documents/> в разделе «Методические рекомендации, инструкции, памятки»)).
4. ИС МФО отправляет ответ в web-версию МП МФО с идентификатором сессии верификации (Sid), мнемоникой системы (InitiatorSystem), ОГРН контрагента (OGRN), адрес возврата пользователя в web-версию МП МФО (ReturnUrl), базовый URL доступа к API Адаптера (AdapterUri).
5. Web-версия МП МФО наполняет обязательными параметрами deeplink (см. п. 1.4) и выполняет переход по нему. При переходе проверяется наличие установленного на устройстве ФЛ МП «Госуслуги Биометрия» и в случае его отсутствия выполняется перенаправление пользователя в соответствующий магазин приложений на страницу МП «Госуслуги Биометрия». При установленном МП «Госуслуги Биометрия» осуществляется переход по deeplink в мобильное приложение.
6. МП «Госуслуги Биометрия» проверяет наличие обязательных параметров в deeplink. Если проверка не пройдена, пользователю отображается экран ошибки с возможностью возврата в мобильную web-версию приложения МФО в случае, если был указан параметр ReturnUrl.
7. МП «Госуслуги Биометрия» выполняет алгоритм авторизации в ЕСИА.

8. После успешного ввода логина и пароля пользователем в ЕСИА, МП «Госуслуги Биометрия» делает запрос на аутентификацию в Инфраструктуре ЕСИА (с прохождением через Инфраструктуру Адаптера и запросом на доступ к ГИС ЕБС). После успешной аутентификации, ЕСИА передает результат с параметрами code1 и state в МП «Госуслуги Биометрия».¹

9. МП «Госуслуги Биометрия» выполняет запрос в Адаптер на получение доступа к биометрической верификации с параметрами code1 и state.

10. Адаптер возвращает ответ с идентификатором сессии и URL web-формы прохождения удаленной идентификации в МП «Госуслуги Биометрия».

11. После получения идентификатора сессии (session_id) МП «Госуслуги Биометрия» вызывает метод «Согласование методов сбора БО и Liveness» REST-сервиса «API биометрической верификации», с параметрами session_id (идентификатор сессии) и metadata (информация о клиентском приложении и устройстве ФЛ). В ответ на вызов ГИС ЕБС возвращает сообщение, содержащее требуемое действие для проверки «живости» (Liveness).

12. МП «Госуслуги Биометрия» запускает процедуру записи БО.

13. МП «Госуслуги Биометрия» передает полученные БО (видеофайл), путем вызова метода «Прием БО на верификацию» REST-сервиса «API биометрической верификации» с параметрами session_id (идентификатор сессии), metadata (дополнительная метаинформация, временная метка и пр.), БО (видеофайл/файлы).

14. В ответ на вызов Инфраструктура ГИС ЕБС возвращает обобщенный результат прохождения биометрической верификации пользователя (успешно или неуспешно) и уникальный идентификатор (verifyToken) в МП «Госуслуги Биометрия». МП «Госуслуги Биометрия» возвращает в Адаптер полученный результат верификации и verifyToken.

15. Адаптер отдает ссылку МП Госуслуги Биометрия для перенаправления в ЕСИА для получения согласия Пользователя на предоставление Пдн Потребителю БДн.

16. ЕСИА запрашивает у Пользователя разрешение на предоставление ИС-Потребителю БДн доступа к персональным данным.

¹ Реализация взаимодействия МП «Госуслуги Биометрия» с ЕСИА при инициации удаленной идентификации производится согласно актуальной версии документа «Методические рекомендации по использованию Единой системы идентификации и аутентификации» (доступен по адресу <https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia>), с использованием криптографического протокола TLS (в частности, см. Раздел 3 «Аутентификация пользователей через ЕСИА»).

17. Пользователь сервиса подтверждает согласие на передачу персональных данных. ЕСИА передает специальный маркер доступа для получения персональных данных в «МП Госуслуги Биометрия».

18. МП «Госуслуги Биометрия» формирует запрос в Адаптер для получения расширенного результата биометрической верификации и ПДн в рамках созданной сессии с параметрами code2 и state, полученными при выдаче согласия пользователем на передачу персональных данных.

19. Адаптер генерирует параметр res_secret и вместе с расширенным результатом биометрической верификации Пользователя передает в ИС МФО.

20. Адаптер отправляет параметр res_secret в МП «Госуслуги Биометрия».

21. Производится возврат ФЛ на заданный web-ресурс (МФО) по переданному URL в параметре dbo_ko_public_uri в запросе на создание сессии верификации в п. 3, где в query-параметрах указывается res_secret и status=SUCCESS.

Схема процесса удаленной идентификации ФЛ с использованием МП «Госуслуги Биометрия» представлена на Рисунке 1.

1.4. Порядок формирования глубинной ссылки (deeplink) для перехода из web-версии МП МФО в МП «Госуслуги Биометрия»

Глубинная ссылка (deeplink) создается на стороне МФО, с возможностью реализации вызова МП «Госуслуги Биометрия», запуска процесса удаленной идентификации с заданными параметрами, передаваемыми в deeplink, а также возможностью скачать МП «Госуслуги Биометрия», если на устройстве ФЛ оно не было установлено.

Параметры, которые должны быть переданы в deeplink:

Таблица 1. Query

Наименование параметра	Тип данных	Обязательность	Описание
InitiatorSystem	String	Да	Мнемоника системы, запрашивающая прохождение удаленной идентификации через МП Госуслуги Биометрия
OGRN	String	Да	ОГРН контрагента
ReturnUrl	UrlEncode	Да	Адрес, на который необходимо направить пользователя, в случае возникновения ошибок. Например: https%3A%2F%2Fwww.example.ru%2Fperson
AdapterUri	UrlEncode	Да	Базовый URL доступа к API Адаптера: <code>https://{{adapter_url}}/api/v{{version}}</code> , где: <ul style="list-style-type: none">• {{adapter_url}} - имя хоста и (опционально) порт API Адаптера• {{version}} - номер версии API Актуальная версия API: «v1». Формат версии: префикс «v» и целое число.

			Например: https%3A%2F%2Ftest_adapter.ru%2Fadapter%2Fv1
Sid	String	Да	Идентификатор сессии

Таблица 2. Fragment

Наименование параметра	Тип данных	Обязательность	Описание
mfo_verification	String	Да	tag для учета в метриках

Пример глубинной ссылки (deeplink):

[[scheme]://[host][path]:[port]?[query]#fragment]
https://ebs.ru/v1/verification/start?InitiatorSystem=MFO&OGRN=1122247030580&ReturnUrl=https%3A%2F%2Fwww.example.ru%2Fperson&AdapterUri=https%3A%2F%2Ftest_adapter.ru%2Fadapter%2Fv1&Sid=5b9dcd00-71a6-4293-ac6c-f367a2ebef7f#mfo_verification

1.6 Статусы прохождения удаленной идентификации

При возврате пользователя в web-версию МП МФО в процессе прохождения удаленной идентификации могут прийти следующие статусы:

Наименование свойства	Описание
SUCCESS	Пользователь успешно прошел удаленную идентификацию в МП Госуслуги Биометрия
FAILURE	Произошла ошибка в процессе удаленной идентификации в МП Госуслуги Биометрия (приходит с параметром error_code см. 1.7)
CANCEL	Пользователь остановил/закрыл процесс удаленной идентификации в МП Госуслуги Биометрия
REPEAT	Произошла ошибка в процессе удаленной идентификации в МП Госуслуги Биометрия, пользователь запросил повторить верификацию. В данном случае необходимо автоматически начать процесс удаленной идентификации заново в web-версии МП МФО (приходит с параметром error_code см. 1.7)

1.7 Коды ошибок (error_code)

Перечень возможных значений параметра error_code:

error_code	Описание
MOB-000115	Отсутствие обязательного параметра в deeplink
EBS-010001	Внутренняя ошибка API
EBS-010003	Неверный запрос. Ошибка очередности вызова API
EBS-010004	Запрос не содержит обязательного параметра {название параметра}
EBS-010105	Биометрический образец отсутствует
EBS-010106	Присутствует более одного образца
EBS-010107	Не удалось извлечь биометрические признаки
EBS-010108	Ошибка верификации (биометрическая верификация не пройдена)
EBS-010110	Пользователю запрещен доступ в ЕБС
EBS-010111	Не верный формат действий (описание действий не совпадают с отправленными)
EBS-010115	Неверный формат метаданных
EBS-010302	Идентификатор сессии не найден
EBS-010303	Время жизни сессии истекло
EBS-*****	Другие ошибки ЕБС описаны в методических рекомендациях по работе с Единой биометрической системой для разработчиков (последняя версия опубликована по адресу: https://ebs.ru/documents/)
ADR-*****	Ошибки адаптера описаны в руководстве программиста ТИБ (последняя версия опубликована по адресу: https://ebs.ru/documents/tibkriptosdktls/)
ESIA-*****	Ошибки ЕСИА описаны в методических рекомендациях по использованию ЕСИА (последняя версия опубликована по адресу: https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia)