**СИСТЕМА «IDЕСИА. ТИПОВОЕ РЕШЕНИЕ ДЛЯ ВЗАИМОДЕЙСТВИЯ С ЕСИА»**

**Описание API**

2025

Оглавление

[1 Список сокращений 3](#_Toc57914025)

[2 Общие принципы взаимодействия с Модулем 3](#_Toc57914026)

[3 Порядок выполнения функциональных сценариев 3](#_Toc57914027)

[3.1 Функциональный сценарий «Запрос создания сеанса аутентификации пользователя» 3](#_Toc57914028)

[3.2 Функциональный сценарий «Запрос статуса сеанса аутентификации пользователя ЕСИА» 4](#_Toc57914029)

[3.3 Функциональный сценарий «Запрос основной информации и дополнительных сведений о пользователе ЕСИА» 5](#_Toc57914030)

[**Приложение 1. Сообщения об ошибках обмена** 6](#_Toc57914031)

1. Список сокращений

ВИС – внешняя информационная система

ЭП – электронная подпись

Модуль – СИСТЕМА «IDЕСИА. ТИПОВОЕ РЕШЕНИЕ ДЛЯ ВЗАИМОДЕЙСТВИЯ С ЕСИА»

1. Общие принципы взаимодействия с Модулем

Взаимодействие внешней информационной системы (ВИС) с Модулем осуществляется по протоколу TCP в режиме «запрос-ответ». Сообщения представляют собой http-запросы.

Предусмотрены следующие виды сообщений:

* Запрос создания сеанса аутентификации пользователя ЕСИА;
* Ответ на запрос создания сеанса аутентификации пользователя ЕСИА;
* Запрос статуса сеанса аутентификации пользователя ЕСИА;
* Ответ на запрос статуса сеанса аутентификации пользователя ЕСИА.
* Запрос основной информации и дополнительных сведений о пользователе ЕСИА;
* Ответ на запрос основной информации и дополнительных сведений о пользователе ЕСИА.

Для получения основной информации и дополнительных сведений о пользователе ЕСИА ВИС необходимо создать сеанс идентификации пользователя. Для этого ВИС формирует запрос в Модуль, содержащий сгенерированный идентификатор сеанса. Модуль формирует УРЛ запроса к сервису аутентификации пользователей ЕСИА, в том числе ЭП запроса, в соответствии с требованиями Методических рекомендаций ЕСИА и инфраструктуры Цифрового профиля. Список разрешений (permissions) для формирования запроса берется из файла, указанного в настройках в исходном виде. ВИС отправляет полученный запрос, после чего ЕСИА направляет в Модуль данные для получения маркера идентификации, используя переадресацию пользователя. Пользователь при этом перенаправляется на адреса согласно разделу 4. Используя полученные данные, Модуль получает у ЕСИА маркер идентификации и валидирует его. В случае успешной валидации аутентификация считается выполненной.

ВИС осуществляет проверку состояния процесса аутентификации путем отправки Модуль запросов статуса сеанса аутентификации пользователя ЕСИА. В случае, когда статус говорит о том, что аутентификация успешно выполнена, ВИС отправляет в Модуль запрос получения информации и сведений о пользователе, идентичный тому, который был бы направлен ЕСИА для получения информации или сведений о пользователе. Модуль перенаправляет запрос в ЕСИА, получает ответ и передает его в том виде, в котором он был получен.

При взаимодействии с ЕСИА применяются алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

1. Порядок выполнения функциональных сценариев

## Функциональный сценарий «Запрос создания сеанса аутентификации пользователя»

Для передачи запроса создания сеанса аутентификации пользователя ЕСИА через Модуль ВИС формирует запросное сообщение на адрес: …/AuthCreate, используя REST API, метод POST, указывая параметры:

«id» = «Идентификатор сеанса» (сгенерированное значение), обязательно.

«scenario» = «Код сценария», опционально. Соответствует наименованию файла (без расширения «.json»), из которого будут загружены разрешения по сценарию. Файл должен находиться в том же каталоге, что и файл с разрешениями, указанный в настройках. В случае отсутствия параметра, разрешения будут загружены из файла, указанного в настройках.

ВИС получает ответ согласно Табл. 1.

**Табл. 1 Реквизитный состав сообщения «Ответ на запрос создания сеанса аутентификации пользователя» в формате REST JSON**

| **№** | **Наименование реквизита сообщения** | **Кол-во эл-тов** | **Порядок формирования** |
| --- | --- | --- | --- |
|  | id | 0..1 | Идентификатор сеанса  Идентификатор сеанса не будет указан в случае его отсутствия в запросе |
|  | url | 0..1 | URL запроса в адрес ЕСИА  Присутствует в случае успешной обработки запроса |
|  | errorStatusInfo | 0..1 | Ошибка. Контейнер.  Заполняется в случае возникновения ошибки |
|  | code | 1 | Код ошибки |
|  | message | 1 | Описание ошибки |

## Функциональный сценарий «Запрос статуса сеанса аутентификации пользователя ЕСИА»

Для передачи запроса статуса сеанса аутентификации пользователя ЕСИА через Модуль ВИС формирует запросное сообщение на адрес: …/AuthStatus, используя REST API, метод GET, указывая параметр «id» = «Идентификатор сеанса».

ВИС получает ответ согласно **Табл. 2**, при этом, в случае, когда сообщение в адрес Модуля не содержало данных, ВИС получит ответ HTTP 400 (Bad Request); в случае истечения таймаута ожидания модулем ответа от ЕСИА, ВИС получит ответ HTTP 408 (Bad Request).

**Табл. 2 Реквизитный состав сообщения «Ответ на запрос статуса сеанса аутентификации пользователя» в формате REST JSON**

| **№** | **Наименование реквизита сообщения** | **Кол-во эл-тов** | **Порядок формирования** |
| --- | --- | --- | --- |
|  | Status\_code | 0..1 | Код статуса согласно справочнику статусов сеанса аутентификации (см. **Табл. 3**)  Заполняется в случае отсутствия ошибок |
|  | Status\_name | 0..1 | Наименование статуса согласно справочнику статусов сеанса аутентификации (см. **Табл. 3**)  Заполняется в случае отсутствия ошибок |
|  | oid | 0..1 | Идентификатор пользователя ЕСИА |
|  | Marker | 0..1 | Маркер идентификации |
|  | access\_token | 0..1 | Маркер доступа |
|  | Expire | 0..1 | Время прекращения действия маркера |
|  | ReceiveTime | 0..1 | Дата и время получения маркера |
|  | errorStatusInfo | 0..1 | Ошибка. Контейнер.  Заполняется в случае возникновения ошибки (Статус - Ошибка аутентификации) либо в случае отсутсвия в БД записи с совпадающим идентификатором сеанса |
|  | code | 1 | Код ошибки |
|  | message | 1 | Описание ошибки |

**Табл. 3 Состав справочника статусов сеансов аутентификации**

| **№** | **Код статуса** | **Наименование статуса** | **Примечание** |
| --- | --- | --- | --- |
|  | 1 | Новый | Статус после получения запроса создания сеанса аутентификации пользователя |
|  | 2 | Ожидает получения авторизационного кода | Статус после отправки ответа на запрос создания сеанса аутентификации пользователя |
|  | 3 | Получен авторизационный код | Промежуточный статус |
|  | 4 | Закончилось время ожидания авторизационного кода | Финальный неуспешный статус |
|  | 5 | Ошибка аутентификации | Финальный неуспешный статус, возникший вследствие ошибки валидации маркера идентификации от ЕСИА  В ответах не указывается, т.к. присутствует только при возникновении ошибки |
|  | 6 | Аутентификация выполнена | Финальный успешный статус сеанса аутентификации |

## Функциональный сценарий «Запрос основной информации и дополнительных сведений о пользователе ЕСИА»

ВИС формирует URL запроса в ЕСИА согласно указанному в разделе №6.1 Методических рекомендаций по интеграции с инфраструктурой Цифрового профиля (версия 1.7), либо в разделе 7.1 Методических рекомендаций по интеграции с REST API Цифрового профиля (версия 1.35) используя полученный в ответе на запрос статуса сеанса аутентификации реквизит «Идентификатор пользователя ЕСИА». ВИС направляет запрос Модулю, метод GET, на адрес …/ClientInfo, содержащего параметр «url», в котором указан URL запроса в ЕСИА. Значение параметра «url» равно значению параметра Path в соответствующем разделе Руководства пользователя, при этом вместо oid требуется указывать идентификатор сеанса пользователя. При получении запроса на стороне модуля идентификатор сеанса будет заменен на идентификатор пользователя, извлеченный из маркера идентификации. Остальная часть запроса останется без изменений и запрос будет направлен в ЕСИА. Например, для получения основных данных о пользователе, согласно разделу 7.1.1 «Основные сведения о гражданине» МР REST API Цифрового Профиля, используется Path: /digital/api/public/{version}/pso/{oid}, где oid – идентификтор пользователя ЕСИА.

Пример значения параметра «url» в запросе ВИС: «/digital/api/public/v1/pso/1234/», где «1234» - идентификатор сеанса.

Соответственно, для получения сведений из документов пользователя, ВИС формирует запрос с параметром «url» согласно указанному в разделе 7.1.2 Коллекция ссылок на документы, после чего формирует запрос с параметром «url» согласно указанному в разделе 7.1.3 Данные документа. Аналогично с прочими запросами, указанными в методических рекомендациях Цифрового Профиля.

ВИС получает ответ полностью идентично полученному от ЕСИА. В случае ошибок обращения к ЕСИА, получения маркера доступа получает ответ от Модуля согласно **Табл. 4**.

**Табл. 4 Реквизитный состав сообщения «Ответ на запрос получения сведений о пользователе в случае ошибки» в формате REST JSON**

| **№** | **Наименование реквизита сообщения** | **Кол-во эл-тов** | **Порядок формирования** |
| --- | --- | --- | --- |
|  | errorStatusInfo | 1 | Ошибка. Контейнер.  Заполняется в случае возникновения ошибки |
|  | code | 1 | Код ошибки |
|  | message | 1 | Описание ошибки |

1. Переадресация пользователя после получения авторизационного кода

После получения авторизационного кода, модуль перенаправляет пользователя на адреса (http-код 302), указанные в настройках «URL успешного результата» или «URL ошибочного результата», содержащий параметры id = Идентификатор сеанса (см. раздел 3.1), и, в случае ошибки, параметр error = Сообщение об ошибке ЕСИА, либо текст «internal\_error» в случае внутренней ошибки модуля.

1. Хеширование сертификата системы клиента (настройка «Хеш сертификата» Версия: v2)

С появлением новых версий «Получение авторизационного кода» и «Получение маркера идентификации» появился новый реквизит client\_certificate\_hash – «это параметр, содержащий хэш сертификата (fingerprint сертификата) системы-клиента в HEX-формате. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к УЗ системы-клиента в ЕСИА.»

Для получения хэш сертификата требуется использовать специализированную утилиту http://esia.gosuslugi.ru/public/calc\_cert\_hash\_unix.zip;

Пример запуска утилиты:

|  |
| --- |
| cpverify.exe test.cer -mk -alg GR3411\_2012\_256 -inverted\_halfbytes 0 |

**Приложение 1. Сообщения об ошибках обмена**

| **№** | **Код ошибки**  **(code)** | **Сообщение об ошибке**  **(message)** | **Примечание** |
| --- | --- | --- | --- |
|  | 100 | Некорректный формат документа | Запрос пуст. |
|  | 105 | Отсутствуют необходимые сведения | В запросе не указан обязательный реквизит. |
|  | 200 | Общая системная ошибка <…> | Неклассифицированная системная ошибка.  Сообщение может содержать дополнительную информацию об ошибке. |
|  | 300 | Невозможно получить токен доступа | Ошибка получения токена доступа в ЕСИА. В случае получения http-кода ответа соответствующего ошибке требуется указывать его. |
|  | 301 | Ошибка отправки запроса в ЕСИА: нет доступа | Невозможно получить ответ от сервера ЕСИА.  В случае получения http-кода ответа соответствующего ошибке требуется указывать его. |
|  | 302 | Истекло максимальное время ожидания обработки сообщения внешней системой <…> | Истекло максимальное время ожидания обработки сообщения.  Сообщение может содержать дополнительную информацию об ошибке. |
|  | 402 | Некорректный статус документа | Документ находится в статусе, не преждусматривающем обработку сообщения. |
|  | 403 | Документ отсутствует в системе | Документ не найден в системе.  Документ, на который ссылается запрос, не найден в системе. |
|  | 404 | Документ уже присутствует в системе | Загружаемый документ уже присутствует в системе. |