

# Инструкция по интеграции с методами ЕСИА для авторизации пользователей в региональном электронном журнале и дневнике

## Аннотация

Данная инструкция описывает порядок применения методов ЕСИА для корректной авторизации пользователей в региональном электронном журнале и дневнике с помощью учётных записей портала Госуслуг. Корректная реализация описанного здесь порядка обеспечивает успешную авторизацию в ЭЖД как учеников, так и их родителей.

## Термины и сокращения

Термин / Сокращение	Определение
ЕГР ЗАГС	Единый государственный реестр записей актов гражданского состояния
ЕПГУ, портал Госуслуг	Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»
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»
ПС, Платформа согласий	Программная среда исполнения ЕСИА, обеспечивающая доступ внешним ИС к персональным данным только при наличии выданного субъектом персональных данных согласия для конкретной ИС организации
СНИЛС	Страховой номер индивидуального лицевого счёта в системе государственного пенсионного страхования Российской Федерации
СОР	Свидетельство о рождении
УЗ	Учётная запись
ФИО	Фамилия, имя и отчество

Термин / Сокращение	Определение
ЭЖД	Региональный электронный журнал и дневник
API	Программный интерфейс приложения, интерфейс прикладного программирования (англ. application programming interface) - описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой
oid	Идентификатор УЗ в ЕСИА
REST	Архитектурный стиль взаимодействия компонентов распределённого приложения в сети

## Ссылки на документы

Документ	Ссылка
Методические рекомендации по интеграции с REST API Цифрового профиля	<a href="https://digital.gov.ru/ru/documents/7166/">https://digital.gov.ru/ru/documents/7166/</a>
Методические рекомендации по использованию Единой системы идентификации и аутентификации	<a href="https://digital.gov.ru/ru/documents/6186/">https://digital.gov.ru/ru/documents/6186/</a>
Регламент информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства	<a href="https://digital.gov.ru/ru/documents/4244/">https://digital.gov.ru/ru/documents/4244/</a>

## Сценарии взаимодействия

Участники взаимодействия:

- Пользователь;
- ЭЖД;

- ЕСИА;
- Платформа согласий.

В качестве Пользователя выступает ученик или его родитель.

### **Сценарий авторизации ученика младше 18 лет**

Для авторизации ученика младше 18 лет пользовательский путь выглядит следующим образом:

- Родитель в ЛК на портале Госуслуг в разделе «Семья и дети» (<https://lk.gosuslugi.ru/profile/family>) заполняет данные по своему ребёнку;
- Родитель дожидается проверки данных о ребёнке в ЕГР ЗАГС;
- Родитель в этом же разделе создаёт детскую учётную запись ребёнка;
- Если в регионе доступна услуга «Школьное портфолио», то родитель может выдать согласие на передачу персональных данных своего ребёнка для его авторизации в ЭЖД посредством соответствующей функции раздела;
- Если в регионе недоступна услуга «Школьное портфолио», то выдача согласия осуществляется в 2 шага:
  - Ребенок авторизуется в ЭЖД с помощью своей (детской) УЗ портала Госуслуг. Авторизация будет неуспешной в связи с отсутствием ранее выданного согласия. Запрос на выдачу согласия будет отображен в ленте уведомлений родителя на портале Госуслуг;
  - Родитель в своём ЛК выдает согласие на передачу персональных данных своего ребенка для его авторизации в ЭЖД;
- Ребёнок авторизуется в ЭЖД с помощью своей (детской) УЗ портала Госуслуг.

При наличии выданного родителем согласия и до его отзыва родителем ребёнок сможет авторизоваться в ЭЖД. При успешной авторизации ребёнка для целей корректного сопоставления реквизитов УЗ портала Госуслуг и УЗ ЭЖД из ЕСИА передаются следующие подтверждённые данные пользователя:

- ФИО;
- Дата рождения;
- Контактные данные (телефон, адрес электронной почты);
- СНИЛС;
- Данные паспорта (при наличии);
- Данные свидетельства о рождении (СОР).

Рекомендуется проверить / обновить СНИЛС и oid ученика на стороне ЭЖД. В случае если сопоставить УЗ портала Госуслуг и УЗ ЭЖД на стороне ЭЖД не представляется возможным (например, опечатка в ФИО, некорректно указаны СНИЛС или СОР), необходимо с помощью средств ЭЖД сформировать обращение гражданина в учебное заведение (проинформировать учебное заведение о необходимости скорректировать данные учетной записи ЭЖД), обработать его и предоставить ответ.

### **Сценарий авторизации ученика старше 18 лет**

Для авторизации ученика (старше 18 лет) пользовательский путь выглядит следующим образом:

- Ученик авторизуется в ЭЖД с помощью своей (подтверждённой) УЗ портала Госуслуг;
- При первой авторизации у ученика будет запрошено согласие на передачу своих персональных данных для авторизации в ЭЖД.

При наличии выданного согласия и до его отзыва ученик сможет авторизоваться в ЭЖД.

При успешной авторизации для целей корректного сопоставления реквизитов УЗ портала Госуслуг и УЗ ЭЖД из ЕСИА передаются следующие подтверждённые данные пользователя:

- ФИО;
- Дата рождения;
- Контактные данные (телефон, адрес электронной почты);
- СНИЛС;
- Данные паспорта;
- Данные свидетельства о рождении (при наличии).

Рекомендуется проверить / обновить СНИЛС и oid ученика на стороне ЭЖД. В случае если сопоставить УЗ портала Госуслуг и УЗ ЭЖД на стороне ЭЖД не представляется возможным (например, опечатка в ФИО, некорректно указаны СНИЛС или СОР), необходимо с помощью средств ЭЖД сформировать обращение гражданина в учебное заведение (проинформировать учебное заведение о необходимости скорректировать данные учетной записи ЭЖД), обработать его и предоставить ответ.

### **Сценарий авторизации родителя**

Для авторизации родителя пользовательский путь выглядит следующим образом:

- Родитель авторизуется в ЭЖД с помощью своей (подтверждённой) УЗ портала Госуслуг;
- При первой авторизации у родителя будет запрошено согласие на передачу своих персональных данных для авторизации в ЭЖД. Данные детей, заполненные в профиле родителя, относятся к персональным данным родителя и, при наличии согласия, также передаются в ЭЖД для целей корректного формирования учётной записи родителя и связывания УЗ родителя и его детей в ЭЖД.

При наличии выданного согласия и до его отзыва родитель сможет авторизоваться в ЭЖД.

При успешной авторизации для целей корректного сопоставления реквизитов УЗ портала Госуслуг и УЗ ЭЖД из ЕСИА передаются следующие подтверждённые данные пользователя:

- ФИО;
- Дата рождения;
- Контактные данные (телефон, адрес электронной почты);
- СНИЛС;
- Данные паспорта;
- Список детей со следующими данными:
  - ФИО;
  - Дата рождения;
  - СНИЛС;
  - Пол;
  - Контактные данные.

Обращаем внимание, что данные свидетельства о рождении ребёнка в списке детей не передаются. Для сопоставления УЗ по данным СОР необходима авторизация с помощью детской УЗ.

Рекомендуется проверить / обновить СНИЛС и oid родителя на стороне ЭЖД, а также выполнить связывание УЗ родителя и учеников на стороне ЭЖД. В случае если сопоставить УЗ портала Госуслуг и УЗ ЭЖД на стороне ЭЖД не представляется возможным (например, опечатка в ФИО, некорректно указаны СНИЛС или СОР), необходимо порекомендовать либо авторизоваться в ЭЖД с помощью детской УЗ (для

связывания по СОР), либо с помощью средств ЭЖД сформировать обращение гражданина в учебное заведение (проинформировать учебное заведение о необходимости скорректировать данные учетной записи ЭЖД), обработать его и предоставить ответ.

Родительскую УЗ в случае ошибки связывания с УЗ родителя портала Госуслуг можно создать, заполнив данными, полученными при авторизации, и привязав к УЗ учеников со стороны ЭЖД.

### Интеграция ЭЖД с ЕСИА

Порядок взаимодействия и вызова методов ЕСИА для авторизации пользователя представлен на диаграмме последовательности.

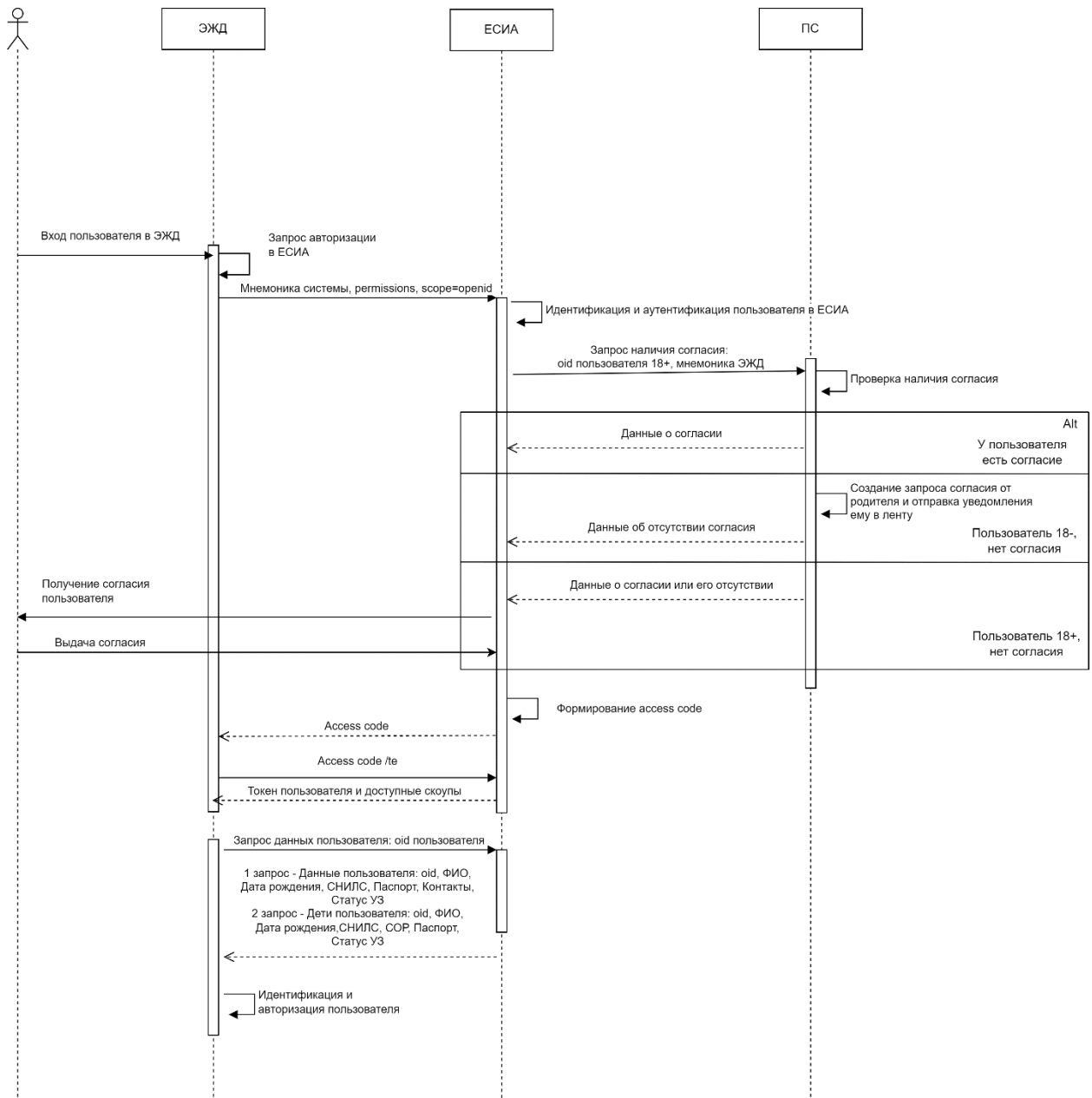


Рисунок 1 - Порядок взаимодействия и вызова методов ЕСИА

Для успешной авторизации пользователя в ЭЖД пользователю необходимо предоставить согласие в личном кабинете (ЛК) на портале Госуслуг. Там же пользователь может видеть и отзывать выданные ранее согласия. Управляет выдачей и отзывом согласий на авторизацию с помощью детской учётной записи родитель ученика. При авторизации пользователя проверка наличия выданного согласия происходит на стороне ЕСИА. Для формирования запроса выдачи согласия в ЛК родителя ученика на портале Госуслуг ученику необходимо предпринять попытку авторизации в ЭЖД с использованием детской учётной записи ЕСИА. После этого в ЛК родителя появится уведомление о запросе согласия на предоставление данных в ЭЖД. В случае если родитель выдаст согласие на предоставление данных, ученик сможет авторизоваться в ЭЖД с помощью своей (детской) учётной записи ЕСИА вплоть до своего совершеннолетия, либо до отзыва ранее выданного согласия родителем в своем ЛК портала Госуслуг.

Срок выдачи согласия родителем для ребёнка автоматически ограничен датой наступления совершеннолетия ребенка.

При отсутствии согласия для пользователя 18 лет и старше на стороне ЕСИА будет формироваться запрос согласия, которое пользователь должен будет выдать.

При отсутствии согласия для пользователя младше 18 лет на стороне ЕСИА будет сформирован и направлен запрос согласия родителю в ЛК ЕПГУ. В системе ЭЖД необходимо при этом отображать баннер с текстом: «Для входа в электронный дневник необходимо согласие. Если вам больше 18 лет, перейдите по ссылке из уведомления, направленного в ваш личный кабинет. Если меньше, перейти по ссылке из своего личного кабинета для выдачи согласия должен родитель». В таком случае в токене возвращается только скоуп: `openid`.

Если согласие было выдано, ЭЖД может использовать методы ЕСИА для сопоставления учетных записей ЕСИА и ЭЖД (в токене содержатся описанные скоупы).

В случае если ЭЖД использует другой набор скоупов, владельцу ИС необходимо заполнить заявку из Регламента по изменению параметров подключения (Приложение Д к Регламенту ЕСИА), описать там все изменения, а после стандартно направить её в адрес СЦ [sd@sc.digital.gov.ru](mailto:sd@sc.digital.gov.ru). Как только пройдут все этапы согласования, и заявка попадет на 2-ю линию поддержки ЕСИА, она будет обработана, и станут доступны описанные скоупы.

### **Получение авторизационного кода**

Получение авторизационного кода необходимо осуществлять в соответствии с «Методическими рекомендациями по использованию Единой системы идентификации и

аутентификации» (см. Приложение В, п.В.2.3). Дополнительно в запрос необходимо добавить параметр «permissions» в соответствии «Методическими рекомендациями по интеграции с REST API Цифрового профиля» (см. Раздел 4) для получения согласий.

Пример параметра «permissions» в кодированном виде Base64 format:

W3sKICAgICAgICAic2NvcGVzIjogW3sKICAgICAgICAgICAgICJzeXNuYW1lI  
jogImZlbgXuYW1lIlgogICAgICAgICAgICB9LCB7CiAgICAgICAgICAgICAgICAic3lzbmFtZ  
SI6ICJiaXJ0aGRhdGUiCiAgICAgICAgICAgICAgIH0sIHsKICAgICAgICAgICAgICAgICJzeXNuY  
W1lIjogInNuaWxzIgogICAgICAgICAgICB9LCB7CiAgICAgICAgICAgICAgICAgICAic3lzbmFtZS  
I6ICJpZF9kb2MiCiAgICAgICAgICAgICAgIH0sIHsKICAgICAgICAgICAgICAgICJzeXNuYW1lIjo  
gImVtYWlsIlgogICAgICAgICAgICB9LCB7CiAgICAgICAgICAgICAgICAgICAic3lzbmFtZSI6ICJt  
b2JpbGUiCiAgICAgICAgICAgICAgIH0sIHsKICAgICAgICAgICAgICAgICJzeXNuYW1lIjogImJpc  
nRoX2Nlc nRfZG9jIlgogICAgICAgICAgICB9LCB7CiAgICAgICAgICAgICAgICAgICAic3lzbmFtZ  
SI6ICJlc3Jfc mVnX2N4dCIKICAgICAgICAgICAgfSwgewogICAgICAgICAgICAgICAgICAgInN5c  
25hbWUiOiAia2lkX2VtYWlsIlgogICAgICAgICAgICB9LCB7CiAgICAgICAgICAgICAgICAgICAic  
3lzbmFtZSI6ICJraWRfbW9iaWxlIlgogICAgICAgICAgICB9LCB7CiAgICAgICAgICAgICAgICAgI  
CAic3lzbmFtZSI6ICJraWRfZnVs bG5hbWUiCiAgICAgICAgICAgICAgIH0sIHsKICAgICAgICAgIC  
CAgICAgICJzeXNuYW1lIjogImtpZF9zbmlscyIKICAgICAgICAgICAgfSwgewogICAgICAgIC  
AgICAgICAgICAgInN5c25hbWUiOiAia2lkX2Jpc nRoZGF0ZSIKICAgICAgICAgICAgfSwgewogIC  
AgICAgICAgICAgICAgICAgInN5c25hbWUiOiAia2lkX2dlbmRlciIKICAgICAgICAgICAgfQogICA  
gICAgIF0sCiAgICAgICAgICAgInN5c25hbWUiOiAiRURVX0pPVVJOQUwiLAogICAgICAgICJw  
dXJwb3NlcyI6IFt7CiAgICAgICAgICAgICAgICAgICAic3lzbmFtZSI6ICJFRFVfSk9VUk5BTCIKIC  
AgICAgICAgICAgfQogICAgICAgIF0sCiAgICAgICAgICAgImFjdGlbnMiOiBBewogICAgICAgIC  
AgICAgICAgICAgInN5c25hbWUiOiAiQUxMX0FDVEIPTINFVE9fREFUQSIIKICAgICAgICAgIC  
AgfQogICAgICAgIF0sCiAgICAgICAgICAgInJlc3BvbnNpYmxlT2JqZWNOIjogItCh0LXQutGAOL  
XRgtCw0YDRjCl sCiAgICAgICAgICAgImV4c GlyZSI6IDI2Mjk3NDYwCiAgICB9Cl0K

Пример в декодированном виде:

```
[{
  "scopes": [{
    "sysname": "fullname"
  }, {
    "sysname": "birthdate"
  }, {
```



```

        "sysname": "snils"
    }, {
        "sysname": "id_doc"
    }, {
        "sysname": "email"
    }, {
        "sysname": "mobile"
    }, {
        "sysname": "birth_cert_doc"
    }, {
        "sysname": "usr_reg_cxt"
    }, {
        "sysname": "kid_email"
    }, {
        "sysname": "kid_mobile"
    }, {
        "sysname": "kid_fullname"
    }, {
        "sysname": "kid_snils"
    }, {
        "sysname": "kid_birthdate"
    }, {
        "sysname": "kid_gender"
    }
],
"sysname": "EDU_JOURNAL",
"purposes": [{
    "sysname": "EDU_JOURNAL"
}],
"actions": [{
    "sysname": "ALL_ACTIONS_TO_DATA"
}],
"responsibleObject": "Секретарь",

```

```
"expire": 26297460
}
]
```

При запросе авторизационного кода на стороне ЕСИА будет обеспечено выполнение проверки наличия согласия на передачу данных пользователя из ЕСИА в ЭЖД. Для пользователей 18 лет и старше будет выполняться проверка согласия от самого пользователя, для пользователей младше 18 лет будет выполняться проверка наличия согласия от одного из родителей (пользователей ЕПГУ, у которых в ЕСИА установлена связь с учетной записью ребенка).

Если согласие выдано на все необходимые скоупы данных, для родителя ЕСИА вернёт в ответе следующие скоупы:

- fullname?oid={p.prn\_oid};
- birthdate?oid={p.prn\_oid};
- snils?oid={p.prn\_oid};
- id\_doc?oid={p.prn\_oid};
- email?oid={p.prn\_oid};
- mobile?oid={p.prn\_oid};
- birth\_cert\_doc?oid={p.prn\_oid};
- usr\_reg\_cxt?oid={p.prn\_oid};
- kid\_email?oid={p.prn\_oid};
- kid\_mobile?oid={p.prn\_oid};
- kid\_fullname?oid={p.prn\_oid};
- kid\_snils?oid={p.prn\_oid};
- kid\_birthdate?oid={p.prn\_oid};
- kid\_gender?oid={p.prn\_oid}.

Если родитель не дал согласие, то в токене возвращается скоуп: openid. В таком случае необходимо отображать пользователю баннер «Для входа в электронный дневник необходимо согласие. Если вам больше 18 лет, перейдите по ссылке из уведомления, направленного в ваш личный кабинет. Если меньше, перейти по ссылке из своего личного кабинета для выдачи согласия должен родитель».

Если вошел ребенок, но согласие ещё не выдано, то в токене возвращается скоуп: openid.

Если вошел ребенок (во второй раз, а родитель уже дал согласие), то в токене возвращаются скоупы:

- fullname?oid={p.prn\_oid};
- birthdate?oid={p.prn\_oid};
- snils?oid={p.prn\_oid};
- id\_doc?oid={p.prn\_oid};
- email?oid={p.prn\_oid};
- mobile?oid={p.prn\_oid};
- birth\_cert\_doc?oid={p.prn\_oid};
- usr\_reg\_cxt?oid={p.prn\_oid}.

Обратите внимание, что из скоупов автоматически удалены скоупы с приставкой «kid\_», предназначенные для получения сведений о детях пользователя.

## Получение маркера доступа

Получение маркера доступа в обмен на авторизационный код необходимо осуществлять в соответствии с «Методическими рекомендациями по использованию Единой системы идентификации и аутентификации» (см. Приложение В, п.В.2.5) и «Методическими рекомендациями по интеграции с REST API Цифрового профиля» (см. Раздел 4).

Пример маркера доступа, получаемого в ответе:

JSON Web Token

```
{
  "header": {
    "ver": 1,
    "typ": "JWT",
    "sbt": "access",
    "alg": "RS256"
  },
  "claims": {
    "nbf": 1672240108,
    "permissions": "DIGITAL_OFFER_EDU_JOURNAL_MEJVED_ZAPROS",
    "scope": " fullname?oid={p.prn_oid}
birthdate?oid={p.prn_oid}"
  }
}
```

```

snils?oid={p.prn_oid}
id_doc?oid={p.prn_oid}
email?oid={p.prn_oid}
mobile?oid={p.prn_oid}
birth_cert_doc?oid={p.prn_oid}
usr_reg_cxt?oid={p.prn_oid}
kid_email?oid={p.prn_oid}
kid_mobile?oid={p.prn_oid}
kid_fullname?oid={p.prn_oid}
kid_snils?oid={p.prn_oid}
kid_birthdate?oid={p.prn_oid}
kid_gender?oid={p.prn_oid}
",
  "iss": "http://esia-dev-k8s.test.gosuslugi.ru/",
  "urn:esia:sid": "f1d8c20a-8b56-0cdd-93cd-26e949a27834",
  "urn:esia:sbj_id": 1077484040,
  "exp": 1672243708,
  "iat": 1672240108,
  "client_id": "PGU",
  "permissions_url": "https://esia-dev-k8s.test.gosuslugi.ru/esia-
rs/api/public/v1/prns/1077484040/issued/permissions"
}
}

```

## Получение сведений по родителю

Полученный маркер доступа с OID родителя ЭЖД может использовать для API-методов:

- Получение основных сведений о гражданине  
GET /esia-rs/api/public/v4/prns/{oid\_родителя}?embed=(documents.elements,addresses.elements,contacts.elements)
- Получение перечня детей пользователя  
GET /esia-rs/api/public/v4/prns/{oid\_родителя}?embed=(kids.elements)

- Получение основных сведений о ребенке (по OID родителя и ID ребенка)  
GET /esia-rs/api/public/v4/prns/{oid\_родителя}/kids/{id\_ребенка}?  
embed=(documents.elements,addresses.elements,contacts.elements)
- Получение выданных согласий (с OID родителя)  
GET /esia-rs/api/public/v1/prns/{oid\_родителя}/issued/permissions

### **Получение сведений по ребёнку**

Полученный маркер доступа с OID ребёнка (при входе ребёнка) ЭЖД может использовать для API-методов:

- Получение основных сведений о гражданине  
GET /esia-rs/api/public/v4/prns/{oid\_ребенка}?  
embed=(documents.elements,addresses.elements,contacts.elements)
- Получение выданных согласий (с OID родителя)  
GET /esia-rs/api/public/v1/prns/{oid\_ребенка}/issued/permissions

### **Сообщения об ошибках**

Если авторизовать пользователя 18 лет и старше не удалось, необходимо в ЭЖД отображать баннер: «Ваш дневник не найден. Чтобы решить проблему, \*сообщите о ней через форму обратной связи (ссылка для перехода на форму подачи обращения ПОС)\*».

Если не удалось авторизовать пользователя до 18 лет, необходимо в ЭЖД отображать баннер: «Ваш дневник не найден. Чтобы решить проблему, попросите родителей сообщить о ней через \*форму обратной связи (ссылка для перехода на форму подачи обращения ПОС)\*».