

Повышение уровня авторизации WebSSO с помощью OTP

Оглавление

- # 1. Назначение документа
- # 2. API для виджета отправки OTP.
- # 3. Схема повышения уровня авторизации
- # 4. Общий механизм взаимодействия
 - # 4.1. Редирект
 - # 4.2. Inline
- # 5. Интеграция с виджетом
 - # 5.1. Формат запроса на смену состояния
 - # 5.2. Пример ответа сервера
 - # 5.3. Состояние initiated (только Inline)
 - # 5.4. Состояние send_otp_form
 - # 5.5. Состояние enter_otp_form
 - # 5.6. Перезапуск цепочки в Inline
 - # 5.7. Завершение цепочки
 - # 5.8. Возврат к защищаемому сервису
 - # 5.9. Возможные ограничения на поля формы
 - # 5.10. Возможные коды ошибок

ВАЖНО

Документ предназначен для внутреннего использования

1. Назначение документа

Документ предназначен для разработчиков виджета повышения уровня, описывает сценарий повышения уровня и протокол взаимодействия виджета с сервером. Рекомендуется также ознакомиться с документом "Повышение уровня авторизации" elevation-integration.

2. API для виджета отправки OTP.

Postman коллекция запросов: [otp.json](#) В каждый запрос нужно подставлять текущий execution - идентификатор сессии аутентификации.

3. Схема повышения уровня авторизации

Цветом выделены состояния которые передают управление виджету. Переходы в состояние fail для сокращения не представлены: из всех состояний, которые имеют переход YES, но нет NO, NO ведет на fail.



4. Общий механизм взаимодействия

4.1. Редирект

Повышение уровня авторизации методом редиректа происходит через OAuth 2.0 с передачей параметра auth_level. Если уровень авторизации пользователя меньше запрашиваемого, он будет перенаправлен на виджет повышения уровня по SMS-коду.

Если SMS-код был успешно подтвержден, будет возвращен OAuth 2.0 code, по которому можно получить access_token с повышенным уровнем авторизации auth_level

Токен повышенного уровня авторизации действует фиксированное время (com.rooxteam.sso.auth.level.<authLevel>.ttl секунд, default 40 секунд).

4.1.1. Формат запроса на повышение уровня авторизации

```
GET <sso_host>/sso/oauth2/authorize
  ?response_type=code
  &client_id=ocb_lk
  &realm=%2Fcustomer
  &redirect_uri=http://<sso_host>/sso/secure/lk.jsp
  &auth_level=9
  &method=otp_sms
```

Параметры

- < sso_host > - базовый адрес сервера SSO, например sso.ocb.hosted:8080

имя	обязательный	описание	тип
response_type	да	Параметр OAuth2 (см. RFC 6749)	строка
client_id	да	Параметр OAuth2 (см. RFC 6749)	строка
realm	да	Единица, используемая ОрепАМ, для управления ресурсами	строка
redirect_uri	да	URL обратного редиректа, URL encoded	строка
auth_level	да	Желаемый уровень авторизации для текущего пользователя	число
method	нет	Предпочтительный способ	строка

повышения уровня
авторизации, например
otp_sms

После успешного повышения уровня авторизации OAuth 2.0 /tokeninfo вернет auth_level соответствующий запрашиваемому

Пример:

```
GET <sso_host>/sso/oauth2/tokeninfo?access_token=f67d8b18-7a74-4c8f-bf56-c61ecf7d9f40
```

```
{
  "scope": [
    "telephoneNumber"
  ],
  "realm": "/customer",
  "auth_level": "9",
  "telephoneNumber": "79876543210",
  "token_type": "Bearer",
  "client_id": "ocb_lk",
  "expires_in": 39,
  "access_token": "f67d8b18-7a74-4c8f-bf56-c61ecf7d9f40"
}
```

4.2. Inline

Повышение уровня авторизации методом inline происходит отправкой запроса на рендеринг виджета согласно разделу "Встраивание виджета повышения уровня авторизации inline" документа elevation-integration.

5. Интеграция с виджетом

5.1. Формат запроса на смену состояния

```
POST <sso_host>/sso/auth/otp-sms
Accept: application/json
Content-Type: application/x-www-form-urlencoded
```

ВАЖНО

Параметры обязательные для всех запросов

```
execution:<execution>
_eventId:<_eventId>
```

- <sso_host> - базовый адрес сервера SSO, например sso.rooxteam.com
- <execution> - брать из переданного JSON объекта, параметр execution

- <_eventId> - идентификатор действия, определяется отдельно для каждого состояния

5.2. Пример ответа сервера

```
{
  "step": "send_otp_form",
  "execution": "d31e8d4a-3ee7-4760-b3b6-6cb879...",
  "form": {
    "errors": []
  },
  "serverUrl": "http://sso.ocb.hosted:8080/sso/auth/otp-sms",
  "view": {
    "msisdn": "79876543210",
    "isInline": false
  }
}
```

имя	обязательный	описание	ограничения (constraints)
step	да	Код состояния	всегда send_otp_form
execution	да	Идентификатор предсессии аутентификации	
form.errors	да	Ошибки шага выполнения	
serverUrl	да	URL для следующего запроса	валидный абсолютный URL
view.msisdn	да	Номер телефона, на который будет отправлен OTP SMS	11 цифр, первая всегда 7
view.isInline	да	Признак того, что виджет встроен (inline)	boolean

Результатом выполнения запроса, будет отображение виджета с кнопкой для отправки OTP кода и кнопкой возврата.

5.3. Состояние initiated (только Inline)

Первоначально цепочка в Inline находится в состоянии initiated. Это псевдо-состояние, не требующее какого-либо отображения:

```
{
  "serverUrl": "http://sso.ocb.hosted:8080/sso/auth/otp-sms",
  "step": "initiated",
  "execution": "dec7dacf-as2d-4345-aae5-d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF"
}
```

имя	обязательный	описание	ограничения (constraints)
-----	--------------	----------	---------------------------

имя	обязательный	описание	ограничения (constraints)
serverUrl	да	URL для следующего запроса	
execution	да	Идентификатор предсессии аутентификации	
step	да	Код состояния	всегда initiated

Отправка события start активирует цепочку повышения уровня из этого состояния.

имя	обязательный	описание	констрейнты
_eventId	да	Идентификатор действия	start

5.4. Состояние send_otp_form

Данный шаг отображает виджет с кнопкой для отправки OTP кода и кнопкой возврата.

```
{
  "view": {
    "msisdn": "79876543210",
    "isInline": true
  },
  "serverUrl": "http://sso.ocb.hosted:8080/sso/auth/otp-sms",
  "step": "send_otp_form",
  "execution": "dec7dacf-as2d-4345-aae5-d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF"
}
```

имя	обязательный	описание	ограничения (constraints)
serverUrl	да	URL для следующего запроса	
execution	да	Идентификатор предсессии аутентификации	
step	да	Код состояния	всегда send_otp_form
view.msisdn	да	Номер телефона, на который будет отправлен OTP SMS	11 цифр, первая всегда 7
view.isInline	да	Признак того, что виджет встроен (inline)	boolean

ВАЖНО

Только для Inline: можно вернуть цепочку в это состояние из любого другого с помощью события start (см. раздел "Перезапуск цепочки в Inline").

5.4.1. Отправка кода

имя	обязательный	описание	констрейнты
_eventId	да	Идентификатор действия	send

5.5. Состояние enter_otp_form

```
{
  "form": {
    "errors": [],
    "name": "otpForm",
    "fields": {
      "otpCode": {
        "constraints": [
          {
            "attributes": {
              "regexp": "[0-9]+",
              "flags": []
            },
            "name": "Pattern"
          },
          {
            "name": "NotNull"
          },
          {
            "attributes": {
              "max": 4,
              "min": 4
            },
            "name": "Size"
          }
        ]
      }
    ]
  },
  "view": {
    "otpCodeAvailableAttempts": 3,
    "msisdn": "79876543210",
    "nextOtpPeriod": 120,
    "blockedFor": 0,
    "isBlocked": false
  },
  "serverUrl": "http://sso.ocb.hosted:8080/sso/auth/otp-sms",
  "step": "enter_otp_form",
  "execution": "ec7dacf-as2d-4345-aae5-d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF..."
}
```

имя	обязательный	описание	ограничения (constraints)
serverUrl	да	URL для следующего запроса	
execution	да	Идентификатор предсессии аутентификации	

step	да	Код состояния	всегда enter_otp_form
view.msisdn	да	Номер телефона, на который будет отправлен OTP SMS	11 цифр, первая всегда 7
view.otpCodeAvailableAttempts	да	Кол-во попыток ввода OTP кода	int
view.nextOtpPeriod	да	Время в секундах до наступления возможности отправки нового OTP кода	секунды
view.isBlocked	да	Признак блокировки пользователя	boolean
view.blockedFor	да	Время до разблокировки в секундах, игнорировать если view.isBlocked == false	long
form.errors[].message	нет	Сообщение об ошибке валидации	
form.errors[].field	нет	Поле в котором найдена ошибка	
constraints	нет	Ограничения на поля формы	
constraints.name	нет	Название ограничения поля формы, обязательно для каждого ограничения	
constraints.attributes	нет	Атрибуты ограничения формы	
constraints.attributes.regexp	нет	Регулярное выражение (обязательно для ограничения Pattern)	
constraints.attributes.flags	нет	Флаги регулярного выражения (обязательно для ограничения Pattern)	
constraints.attributes.min	нет	Минимальное значение длины поля (обязательно для ограничения Size)	
constraints.attributes.max	нет	Максимальное значение длины поля (обязательно для ограничения Size)	

Пример ошибки валидации OTP

```

{
  "form": {
    "errors": [
      {
        "field": "otpCode",
        "message": "invalid_otp"
      }
    ],
    "name": "otpForm",
    "fields": {
      "otpCode": {
        "constraints": [
          {
            "attributes": {
              "regexp": "[0-9]+",
              "flags": []
            },
            "name": "Pattern"
          },
          {
            "name": "NotNull"
          },
          {
            "attributes": {
              "max": 4,
              "min": 4
            },
            "name": "Size"
          }
        ]
      }
    ]
  },
  "view": {
    "otpCodeAvailableAttempts": 2,
    "msisdn": "79876543210",
    "nextOtpPeriod": 120,
    "blockedFor": 0,
    "isBlocked": false
  },
  "serverUrl": "http://sso.ocb.hosted:8080/sso/auth/otp-sms",
  "step": "enter_otp_form",
  "execution": "dec7dacf-as2d-4345-aae5-d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF"
}

```

5.5.1. Повторная отправка кода

имя	обязательный	описание	констрейнты
_eventId	да	Идентификатор действия	send

5.5.2. Валидация кода

имя	обязательный	описание	ограничения (constraints)
_eventId	да	Идентификатор действия	validate

5.6. Перезапуск цепочки в Inline

Для перезапуска цепочки в Inline необходимо отправить событие start:

имя	обязательный	описание	констрейнты
_eventId	да	Идентификатор действия	start

Его отправка допустима из любого состояния в рамках повышения уровня (initiated, send_otp_form, и т.д.) После получения этого события состояние цепочки будет сброшено к send_otp_form.

5.7. Завершение цепочки

Ответ при успешном или неуспешном завершении цепочки зависит от способа встраивания виджета.

5.7.1. Редирект

Если повышение уровня авторизации производится методом редиректа, при завершении цепочки, независимо от успешности, нужно выполнить редирект, для этого с сервера приходит ответ такого вида:

Пример

```
{
  "step": "redirect",
  "location": "/sso/auth/complete"
}
```

имя	обязательный	описание	констрейнты
step	да	Код состояния	всегда redirect
location	да	URL для редиректа	

Атрибуты ограничения формы Результатом выполнения данного алгоритма будет окончание аутентификации и редирект на вызывающий ресурс согласно используемому протоколу.

5.7.2. Inline

Успешное завершение

Если виджет был встроен inline, при успешном завершении цепочки сервер вернет oauth code. Виджет должен сгенерировать javascript event с именем eventName и передать в него eventData в соответствии с разделом "Встраивание виджета повышения уровня авторизации inline" документа elevation-integration.

```
{
  "step": "event",
  "eventName": "com.rooxteam.otp.success",
  "eventData": {
    "oauth_code": "9bdd5246-7686-44fe-ab1a-7e8c9deacd8f"
  }
}
```

имя	обязательный	описание	констрейнты
step	да	Идентификатор шага	event
eventName	да	Имя события	com.rooxteam.otp.success
eventData	да	Параметры события	
eventData.oauth_code	да	OAuth code с повышенным уровнем	

Неуспешное завершение

Если виджет был встроен inline, при неуспешном завершении цепочки сервер вернет описание ошибки. Виджет должен сгенерировать javascript event с именем eventName и передать в него eventData в соответствии с разделом "Встраивание виджета повышения уровня авторизации inline" документа elevation-integration.

```
{
  "step": "event",
  "eventName": "com.rooxteam.otp.error",
  "eventData": {
    "error": "<error_code>",
    "error_description": "<error_description>"
  }
}
```

имя	обязательный	описание	констрейнты
step	да	Идентификатор шага	event
eventName	да	Имя события	com.rooxteam.otp.error
eventData	да	Параметры события	
eventData.error	да	Код ошибки	
eventData.error_description	да	Описание ошибки	

5.8. Возврат к защищаемому сервису

В виджете должна быть кнопка, по которой пользователь сможет вернуться на страницу защищаемого сервиса, который инициировал аутентификацию. По клику на эту кнопку должен выполняться запрос на сервер следующего вида:

имя	обязательный	описание	констрейнты
_eventId	да	Идентификатор действия	cancel

5.8.1. Редирект

В случае если виджет на отдельной странице, сервер должен вернуть ответ аналогичный успешному завершению

```
{
  "step": "redirect",
  "location": "/sso/auth/complete"
}
```

Необходимо выполнить редирект пользователя на указанный URL.

5.8.2. Inline

Если виджет встроен inline, будет возвращен ответ следующего вида. Виджет должен сгенерировать javascript event с именем eventName и передать в него eventData в соответствии с разделом "Встраивание виджета повышения уровня авторизации inline" документа elevation-integration.

```
{
  "step": "event",
  "eventName": "com.rooxteam.otp.error",
  "eventData": {
    "error": "canceled",
    "error_description": "Canceled by user"
  }
}
```

имя	обязательный	описание	констрейнты
step	да	Идентификатор шага	event
eventName	да	Имя события	com.rooxteam.otp.error
eventData	да	Параметры события	
eventData.error	да	Код ошибки	
eventData.error_description	да	Описание ошибки	

Помимо проксирования серверных ошибок, виджет также может отправлять собственные через систему событий. Клиент может генерировать события любых типов, описанных в разделе "Неуспешное повышение уровня авторизации" документа elevation-integration. Ниже приведен список известных ошибок и соответствующие им коды:

ошибка	значение event.error
Сервер вернул 502, 503, 504	destination_unreachable
Request timeout	destination_unreachable
Запрет запроса (ошибка в настройках CORS)	destination_unreachable
Сервер вернул 500	server_error
Сервер вернул 403	invalid_grant
В ответе нет error JSON	server_error

5.9. Возможные ограничения на поля формы

См. в документе sso-widget-api

5.10. Возможные коды ошибок

код	описание	комментарий
invalid_otp	Неверный OTP код	
error_sending_otp	Ошибка при отправке SMS с кодом	
too_many_sms	Превышен лимит отправки SMS	
too_many_wrong_code	Превышен лимит попыток ввода OTP кода	
may not be null	Поле не может быть пустым	Ошибка валидации
size must be between {min} and {max}	Значение должно быть в заданном диапазоне	Ошибка валидации
required on {field name}	Обязательное поле	Ошибка валидации
must match "{regexp}"	Соответствие регулярному выражению	Ошибка валидации



