

WebSSO Login API



Документ предназначен для внутреннего использования

1. Схема аутентификации

Цветом выделены состояния которые передают управление виджету.

```
@startuml

skinparam state {
    BackgroundColor<<View>> Peru
}

[*] --> initial_check_ip

initial_check_ip: Заблокирован ли IP?
initial_check_ip --> auth_form : YES
initial_check_ip -down-> auto_login : NO

auto_login: пропустить автовход?
auto_login --> do_auto_login : TRY
auto_login -down-> check_auto_login : CHECK
auto_login --> auth_form : SKIP

state do_auto_login <<View>>
do_auto_login: редирект на url автологина
do_auto_login --> check_auto_login : NEXT

check_auto_login: Попытка авто входа.
check_auto_login -down-> send_message : YES
check_auto_login --> auth_form : NO

state auth_form <<View>>
auth_form: Основная форма логина
auth_form --> check_user : NEXT

send_message: Отправить смс-сообщение\n если в ЛК включено оповещение о входе
send_message --> [*]

check_user: Получение статуса пользователя.
check_user --> check_auth : ACTIVE
check_user --> captcha_auth_form : CAPTCHA
check_user -down-> auth_form : BLOCKED

check_auth: Проверка авторизации пользователя.
check_auth --> send_message : YES
check_auth -up-> check_ip : NO
```

```
state captcha_auth_form <<View>>
captcha_auth_form: Основная форма аутентификации
captcha_auth_form -down-> check_captcha : NEXT
captcha_auth_form --> captcha_auth_form : UPDATE_CAPTCHA
```

```
check_ip: Заблокирован ли IP-адрес?
check_ip --> auth_form : YES
check_ip --> check_user_again : NO
```

```
check_captcha: CAPTCHA верная?
check_captcha -down-> check_auth : YES
check_captcha --> check_ip : NO
```

```
check_user_again: Заблокирован ли аккаунт?
check_user_again --> auth_form : ACTIVE
check_user_again --> captcha_auth_form : CAPTCHA
check_user_again --> auth_form : BLOCKED
```

@endum1



Из всех визуальных состояний есть переход "cancel", завершающий цепочку (состояние fail). Не представлено на схеме для сокращения.

2. Точка входа

Все цепочки аутентификации должны начинаться с OAuth 2.0 или OAuth 1.0 endpoint-ов.

Например:

- OAuth 1.0
http://<sso_host>/sso/oauth/userconsole.jsp?oauth_token=http%3A%2F%2F<sso_host>%2Fsso%2Fresources%2F1%2Foauth%2Ftoken%2Fef16234b5ad44ab89c465661ec8bd442
- OAuth 2.0
http://<sso_host>/sso/oauth2/authorize?response_type=code&realm=/customer&client_id=mgf_lk&redirect_uri=http://<sso_host>/sso/secure/lk.jsp&scope=sso/oauth2/authotioType

3. Авто-вход

Перед стандартным входом по логину/паролю может быть сделана попытка автоматического входа с помощью HTTP header enrichment. Для этого пользователь перенаправляется редиректом на HTTP (не HTTPS) endpoint, и в HTTP запрос подмешивается HTTP заголовок x-nokia-msisdn с доверенным идентификатором пользователя. HTTP endpoint пробрасывает его GET-параметром auto-login-jwt. Если идентификатор валидный, происходит автоматический вход.

Можно пропустить авто-вход если передать на вход в цепочку GET-параметр `roox_skipAutoLogin=true`

4. Блокировки

После `com.rooxteam.uidm.captcha.limit` (default 2) неверных попыток ввода пароля для одного и того же логина требуется вводить CAPTCHA. После `com.rooxteam.uidm.block.limit` (default 10) неверных попыток ввода пароля или CAPTCHA для одного и того же логина происходит временная блокировка по логину на `com.rooxteam.uidm.block.seconds` секунд (default 3600 с = 1 час). `com.rooxteam.uidm.block.limit` включает в себя `com.rooxteam.uidm.captcha.limit`, то есть при значениях по умолчанию достаточно 2 неверных вводов пароля и 8 неверных ввода CAPTCHA чтобы заблокироваться. После `com.rooxteam.uidm.auth.fail.ip.block.limit` (default 240) неверных попыток ввода логина/пароля/CAPTCHA с одного и того же IP-адреса в течение `com.rooxteam.uidm.block.ip.count.period.seconds` секунд (default 86400 с = 24 часа) происходит блокировка этого адреса на `com.rooxteam.uidm.block.ip.seconds` секунд (default 86400 с = 24 часа)

5. API для виджета логина.

5.1. Общий механизм взаимодействия

Для аутентификации пользователя по протоколу OAuth будет происходить запрос со стороннего ресурса (например Личный Кабинет) на WebSSO, где взаимодействие WebSSO сервера с виджетом происходит путем встраивания кода виджета (HTML код) в WebSSO страницу через запрос на WRS с передачей параметров встраивания. А так же начальных данных (параметр `up_inputData`) в виде JSON объекта для отрисовки виджета.

Пример начальных данных:

```
{
  "form": {
    "errors": [],
    "name": "loginForm",
    "fields": {
      "username": {
        "constraints": [
          {
            "name": "NotNull"
          },
          {
            "name": "Size",
            "attributes": {
              "min": 10,
              "max": 25
            }
          }
        ]
      }
    }
  },
  {
```

```

        "name": "FilteredSize",
        "attributes": {
            "skip": "([^9+)]([^0-9])",
            "message": "symbols {skip} should be filtered out, and resulting string
should have length between {min} and {max}",
            "min": 10,
            "max": 10
        }
    }
],
},
"password": {
    "constraints": [
        {
            "name": "Size",
            "attributes": {
                "min": 4,
                "max": 1024
            }
        },
        {
            "name": "NotNull"
        }
    ]
}
},
"view": {
    "logoutReason": "idle_timeout",
    "isBlocked": false
},
"serverUrl": "https://sso.rooxteam.com/sso/auth/websso",
"step": "auth_form",
"execution": "dec7dacf-as2d-4345-aae5-
d08410cb8f95_H4sIAAAAAAAN1WTWwcRRYu27GdxE5wEnYF..."
}

```

имя	обязательный	описание	ограничения (constraints)
serverUrl	да	URL для следующего запроса	валидный абсолютный URL
execution	да	Идентификатор предсессии аутентификации	
step	да	Код состояния	всегда auth_form
view	да	Дополнительные данные текущего шага	11 цифр, первая всегда 7

имя	обязательный	описание	ограничения (constraints)
view.msisdn	да	Номер телефона, на который будет отправлен OTP SMS	11 цифр, первая всегда 7
view.otpCodeAvailable Attempts	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	нет	Время до разблокировки в секундах, не передается если view.isBlocked == false	long
view.logoutReason	нет	Причина логута пользователя (см.ниже)	long
form	нет	Если есть параметр form, значит надо будет отрисовать форму с полями (fields) внутри объекта	
form.fields	нет	Список заполняемых данных пользователем	
fields.username	да	Номер телефона	
fields.password	да	Пароль	
form.constraints	нет	Список ограничений на поле	
constraints.name	нет	Название ограничения поля формы, обязательно для каждого ограничения	
constraints.attributes	нет	Атрибуты ограничения формы	

имя	обязательный	описание	ограничения (constraints)
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)	
form.errors[].message	нет	Сообщение об ошибке валидации	
form.errors[].field	нет	Поле в котором найдена ошибка	

5.1.1. Logout Reason

В первоначальных данных для виджета может быть указан параметр `logoutReason`. В этом случае нужно отобразить пользователю сообщение о причине логута и попадания на виджет логина.

Возможные значения: 1. `session_timeout` - Истечение времени сессии 2. `idle_timeout` - Бездействие пользователя в течение определенного времени

5.2. Вход в ЛК

Для аутентификации по OAuth протоколу пользователь будет перенаправлен на страницу входа, где будет отрисован виджет с формой для ввода логина и пароля.

5.3. Форматы запросов и ответов

5.3.1. Формат запроса на смену состояния

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



Параметры обязательные для всех запросов

```
execution:<executionId>
_eventId:<eventId>
```

- <sso_host> - базовый адрес сервера SSO, например sso.rooxteam.com
- <executionId> - брать из переданного JSON объекта, параметр execution
- <eventId> - идентификатор действия, определяется отдельно для каждого состояния (для auth_form и captcha_auth_form нужно передавать next)
 - для запроса новой "капчи" на captcha_auth_form - <eventId> должен быть равен updateCaptcha

5.3.2. Состояние auth_form

Входные данные (от сервера к виджету)

Пример с ошибкой валидации

```
{
  "form": {
    "errors": [
      {
        "message": "size must be not less than 10",
        "field": "username"
      }
    ],
    "name": "loginForm",
    "fields": {
      "username": {
        "constraints": [
          {
            "name": "NotNull"
          },
          {
            "name": "Size",
            "attributes": {
              "min": 10,
              "max": 25
            }
          }
        ]
      },
      {
        "name": "FilteredSize",
```

```

        "attributes": {
            "skip": "([^9]*)|([^\d])",
            "min": 10,
            "max": 10
        }
    },
    ],
},
"password": {
    "constraints": [
        {
            "name": "Size",
            "attributes": {
                "min": 4,
                "max": 1024
            }
        },
        {
            "name": "NotNull"
        }
    ]
}
},
"view": {
    "isBlocked": false
},
"serverUrl": "https://sso.rooxteam.com/sso/auth/websso",
"step": "auth_form",
"execution": "dec7dacf-as2d-4345-aae5-
d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF..."
}

```

Пример с ошибкой аутентификации

```

{
    "form": {
        "errors": [
            {
                "message": "invalid_credentials"
            }
        ],
        "name": "loginForm",
        "fields": {
            "username": {
                "constraints": [
                    {
                        "name": "NotNull"
                    },
                    {

```

```

        "name": "Size",
        "attributes": {
            "min": 10,
            "max": 25
        }
    },
    {
        "name": "FilteredSize",
        "attributes": {
            "skip": "^(^9*)|(^\\d)",
            "min": 10,
            "max": 10
        }
    }
]
},
"password": {
    "constraints": [
        {
            "name": "Size",
            "attributes": {
                "min": 4,
                "max": 1024
            }
        },
        {
            "name": "NotNull"
        }
    ]
}
},
"view": {
    "isBlocked": false
},
"serverUrl": "https://sso.rooxteam.com/sso/auth/websso",
"step": "auth_form",
"execution": "dec7dacf-as2d-4345-aae5-
d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF..."
}

```

Пример с заблокированным пользователем

```

{
  "form": {
    "errors": [
      {
        "message": "user_blocked"
      }
    ]
  }
}

```

```

"name": "loginForm",
"fields": {
  "username": {
    "constraints": [
      {
        "name": "NotNull"
      },
      {
        "name": "Size",
        "attributes": {
          "min": 10,
          "max": 25
        }
      },
      {
        "name": "FilteredSize",
        "attributes": {
          "skip": "^(^9*)|(^\\d)",
          "min": 10,
          "max": 10
        }
      }
    ]
  },
  "password": {
    "constraints": [
      {
        "name": "Size",
        "attributes": {
          "min": 4,
          "max": 1024
        }
      },
      {
        "name": "NotNull"
      }
    ]
  }
},
"view": {
  "blockedFor": 123456,
  "isBlocked": true
},
"serverUrl": "https://sso.rooxteam.com/sso/auth/websso",
"step": "auth_form",
"execution": "dec7dacf-as2d-4345-aae5-
d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYu27GdxE5wEnYF..."
}

```

Выходные данные (от виджета к серверу)

имя	обязательный	описание	констрейнты
username	да	Номер телефона	набор из символов, минимум 10, максимум 25
password	да	Пароль	4-1024 символа

5.3.3. Состояние captcha_auth_form

Входные данные (от сервера к виджету)

имя	обязательный	описание	констрейнты
serverUrl	да	URL для следующего запроса	
execution	да	Идентификатор предсессии аутентификации	
step	да	Код состояния	всегда captcha_auth_form
view.captchaUrl	да	URL для загрузки капчи	
form.errors[.].message	нет	Сообщение об ошибке валидации	
form.errors[.].field	нет	Поле в котором найдена ошибка	

Пример

```
{
  "form": {
    "errors": [
      {
        "field": "captchaCode",
        "message": "invalid_captcha"
      }
    ],
    "name": "captchaLoginForm",
    "fields": {
      "username": {
        "constraints": [
          {
            "name": "NotNull"
          },
          {

```

```

        "name": "Size",
        "attributes": {
            "min": 10,
            "max": 25
        }
    },
    {
        "name": "FilteredSize",
        "attributes": {
            "skip": "^(^9*)|(^\\d)",
            "min": 10,
            "max": 10
        }
    }
]
},
"captchaCode": {
    "constraints": [
        {
            "name": "Size",
            "attributes": {
                "min": 1,
                "max": 256
            }
        },
        {
            "name": "NotNull"
        }
    ]
},
"password": {
    "constraints": [
        {
            "name": "Size",
            "attributes": {
                "min": 4,
                "max": 1024
            }
        },
        {
            "name": "NotNull"
        }
    ]
}
},
"view": {
    "captchaUrl": "https://sso.rooxteam.com/webapi-3.0/captchas/b6b64f71-cb43-41b8-9df3-e974cdf9a6bf"
},
"serverUrl": "https://sso.rooxteam.com/sso/auth/websso",

```

```

"step": "captcha_auth_form",
"execution": "dec7dacf-as2d-4345-aae5-
d08410cb8f95_H4sIAAAAAAAAAAN1WTWwcRRYU27GdxE5wEnYF..."
}

```

Выходные данные (от виджета к серверу)

имя	обязательный	описание	констрейнты
username	да	Номер телефона	набор из символов, минимум 10, максимум 25
password	да	Пароль	4-1024 символа
captchaCode	да	Код капчи	1-256 символов

5.3.4. Успешное завершение цепочки

Входные данные (от сервера к виджету)

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

Пример

```

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

```

Выходные данные (от виджета к серверу)

Надо сделать редирект на <location>, если он есть и не пустой. Переход на него проставит куку iPlanetAuthToken с временным JWT токеном. После чего пользователь будет перенаправлен на /UI/Login, где ему проставят WebSSO куку и перенаправят на goto.

5.4. Возврат к защищаемому сервису

В виджете может быть кнопка или ссылка, по которой пользователь сможет вернуться на страницу защищаемого сервиса, который инициировал аутентификацию.



Информация о том, отображать ли кнопку, автоматически вызывать cancel при блокировке или просто отображать сообщение, будет пробрасываться в виджет отдельным параметром, детали будут утверждены позже

По клику на эту кнопку или ссылку должен выполняться запрос на сервер следующего

вида:

имя	обязательный	описание	констрейнты
_eventId	да	Идентификатор действия	cancel

Сервер должен вернуть ответ аналогичный успешному завершению

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

Необходимо выполнить редирект пользователя на указанный URL.

5.5. Возможные ограничения на поля формы

название	описание	атрибуты	описание атрибута
NotNull	Обязательность поля		
Size	Длина строкового параметра	min	Минимальная длина
		max	Максимальная длина
Pattern	Regex для строкового параметра	regex	Регулярное выражение
Min	Минимальное значение целого числового параметра	value	Минимальное значение
Max	Максимальное значение целого числового параметра	value	Максимальное значение
DecimalMin	Минимальное значение десятичного числового параметра	value	Минимальное значение
DecimalMax	Максимальное значение десятичного числового параметра	value	Максимальное значение

название	описание	атрибуты	описание атрибута
FilteredSize	Ограничения на номер телефона	min	Минимальная длина
		max	Максимальная длина
		skip	Регулярное выражение для фильтрации. Перед отправкой нужно удалять все, что ему удовлетворяет. Например, происходит очищение введенных данных от всех символов кроме цифр, дальше удалять все символы слева до первой девятки (не включая).

5.6. Возможные коды ошибок

код	описание	комментарий
ip_blocked	Заблокирован IP-адрес	Пока не реализовано
user_blocked	Заблокирован пользователь по данному логину	
invalid_captcha	Неверное значение captcha	
need_captcha	Отсутствует значение captcha	Возникает, когда требуется ввод символов captcha, но они не передаются после начала новой сессии
invalid_credentials	Неверная пара логин/пароль	
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

5.7. Дополнительные условия

Для работы цепочки аутентификации нужно при каждом запросе передавать cookie JSESSIONID. Если cookie отсутствует или истекло время сессии, вернется ошибка HTTP 400

вида:

```
{
  "error": {
    "code": 400,
    "message": "No flow execution could be found with key 'e2s2'"
  }
}
```

Если в запросе указан execution с валидным идентификатором e но невалидным шагом s, вернется ошибка HTTP 400 вида:

```
{
  "error": {
    "code": 400,
    "message": "No flow execution snapshot could be found with id '4'; perhaps the snapshot has been removed?"
  }
}
```