OpenID Connect UserInfo - получение информации о текущем пользователе

Оглавление

Используется для получения информации о пользователе, который представлен токеном доступа.

Примеры:

- отображение базовой информации о пользоваетеле в "шапке" сервиса

Описание механизма

1. Пользователь аутентифицируется некоторым способом, получает токен доступа
2. Frontend или Backend система, желающая получить информацию о текущем пользователе, выполняет вызов конечной точки UserInfo

Конечная точка

```
GET https://{sso_host}/uidm-webapi-1/userinfo
```

или

```
POST https://{sso_host}/uidm-webapi-1/userinfo
```

- Референсная спецификация: OpenID Connect Core 1.0
- Предоставляется сервисом: `customer-webapi`

Получение информации о текущем пользователе

Выполняется HTTP вызов конечной точки с передачей токена доступа.

```
POST /uidm-webapi-1/userinfo
Host: <sso_host>
Accept: application/json
Authorization: Bearer <access_token>
```

- sso_host - базовый адрес сервера WebSSO, например sso.rooxteam.com
- access_token - токен доступа

Формат ответа для валидного токена (не нормативный)

```
HTTP/1.1 200 OK
```

```
{
  "sub": "bis__000000000000",
  "realm": "/customer",
  "roles": [
    "ROLE_SYSTEM"
  ],
  "preferred_username": "79000000000",
  "phone_number": "+79000000000",
  "name": "Jane Doe",
  "given_name": "Jane",
  "family_name": "Doe",
  "email": "janedoe@example.com"
}
```

- sub - идентификатор клиента;
- realm - область пользователей UIDM;
- roles - список ролей присвоенных клиенту;
- auth_level - уровень авторизации пользователя
- preferred_username - логин пользователя

ЗАМЕТКА

Правила обработки ответа: ответ может содержать и другие поля; клиент обязан игнорировать поля, которые он не анализирует. Ответ может не содержать поля в следствии настроек сервера. Обязательным полем является только `sub`. Формат поля phone_number - E.164.

Формат ответа для невалидного токена

Если токен доступа указан неверно, либо его срок действия истёк, конечная точка возвращает ошибку:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: error="invalid_token", error_description="The request contains a token
```

```
no longer valid."
```

- error - строковый код ошибки
- error_description - описание ошибки

Конфигурация сервера, влияющая на содержание ответа

Ключ	Описание	По умолчанию
com.rooxteam.uidm.userinfo.claims_whitelist	Белый список клеймов, разрешенных для отдачи в конечной точке UserInfo	Пустой список*
com.rooxteam.uidm.otp.phone_number_mask.search	Маскирование телефонного номера, регулярное выражение для поиска значения под замену	Не задано, маскирование выключено
com.rooxteam.uidm.otp.phone_number_mask.replace	Маскирование телефонного номера, регулярное выражение для замены значения	Не задано, маскирование выключено
com.rooxteam.uidm.claims.preferred_username.source	Имя атрибута профиля, используемое сервером для вычисления значения клейма preferred_username	user_name

- поскольку конечная точка UserInfo открыта для публичного интернета, для целей безопасности по умолчанию отдается только поле `sub`.
- белый список не включает поле `sub` - оно отдается всегда