

OpenID Connect Discovery - получение информации о конфигурации сервера RooX UIDM

Оглавление

- # Конечная точка
- # Получение информации о конфигурации системы
 - # Формат ответа

Используется для получения конечных точек, открытых ключей и прочей конфигурации, упрощающей настройку серверных систем, которые интегрируются с RooX UIDM.

Примеры:

- получение конечной точки UserInfo
- получение открытого ключа для локальной валидации JWT токена

Описание механизма

1. Система запрашивает конфигурацию
2. Frontend или Backend система, желающая получить информацию о текущем пользователе, выполняет вызов конечной точки UserInfo

Конечная точка

GET https://{sso_host}/sso/.well-known/openid-configuration

- Референсная спецификация: [OpenID Connect Discovery 1.0](#)
- Предоставляется сервисом: `sso-server`

ЗАМЕТКА

Спецификация требует, чтобы `.well-known` адрес располагался сразу после issuer. В типовой конфигурации issuer выглядит как `https://sso.hostname.com/sso`, то есть содержит компоненту пути. Это не является нарушением спецификации Discovery.

Получение информации о конфигурации системы

Выполняется HTTP вызов конечной точки.

```
GET /sso/.well-known/openid-configuration
Host: <sso_host>
```

- sso_host - базовый адрес сервера RooX UIDM, например sso.rooxteam.com

Формат ответа

HTTP/1.1 200 OK

```
{
  "issuer": "https://{sso_host}/sso",
  "authorization_endpoint": "https://{sso_host}/sso/authorize",
  "token_endpoint": "https://{sso_host}/sso/token",
  "userinfo_endpoint": "https://{sso_host}/sso/uidm-webapi-1/userinfo",
  "jwks_uri": "https://{sso_host}/sso/jwks.json",
  "response_types_supported": [
    "code",
    "id_token",
    "mpt"
  ],
  "subject_types_supported": [
    "public"
  ],
  "id_token_signing_alg_values_supported": [
    "HS512",
    "RS512"
  ]
}
```

- sso_host - публичный адрес сервера RooX UIDM (балансировщика);
- authorization_endpoint - URL конечной точки аутентификации через OAuth Code Grant
- token_endpoint - URL конечной точки получения токена
- userinfo_endpoint - URL конечной точки информации о пользователе
- jwks_uri - URL описания ключей - JWKS
- id_token_signing_alg_values_supported - доступные алгоритмы подписания JWT токенов

ЗАМЕТКА

Правила обработки ответа: ответ может содержать и другие поля; клиент обязан игнорировать поля, которые он не анализирует.

