

OpenID Connect

Identidade virtual

Motivação

Evento : Simpósio de Segurança Computacional

Tema : OpenID Connect

Local : Rio de Janeiro - RJ

Data : 10/10/13

Sua expectativa : "Não posso perder!"

Planejamento

1. Inscrever-se no evento
2. Comprar passagem de avião
3. Buscar bons hotéis
4. Comprar uma mala grande e barata

Organização do Evento

Provide your personal information

* Given/First name:

Middle name:

* Last/Family/Surname:

Enter e-mail address & password

The e-mail address provided here will be the username of your account.

* E-mail address:

* Re-enter e-mail address:

* Password:

* Confirm password:

Password Strength

Passwords must be between 8 and 64 characters, and include at least one number. [More...](#)

Set security questions

For your security, IEEE Accounts are required to have two security questions and answers.

* Security question 1:

* Type your answer:

* Security question 2:

* Type your answer:



CIA Aviação



DADOS PESSOAIS ↗

2 LOGIN E CONTATO ↗

3 COMPLEMENTOS ↗

PREFERÊNCIAS DE NAVEGAÇÃO:

Idioma de preferência:*

Português ▼

Nacionalidade:*

BRASIL ▼

MEUS DADOS

*Campos de preenchimento obrigatório.

Nome Completo:*

Como você quer ser chamado?:*

Seu nome como aparecerá no cartão:*

CPF:*

CPF:*

CPF próprio?*



Sim



Não

Profissão:

Data de nascimento:*

Dia:

Mês:

Ano:

Estado civil:*

Número de Filhos:

DADOS PROFISSIONAIS

Busca de Hotéis



Endereço de e-mail

Senha

De 6 a 20 letras, com no mínimo 1
número

Confirmar senha

De 6 a 20 letras, com no mínimo 1
número

Nome

Sobrenome

Código postal

País

Brasil

Telefone

Moeda preferida

BRL Real (R\$)

Welcome Rewards

Ao se inscrever na Hoteis.com, você receberá 1 diária GRÁTIS para cada 10 noites de estadia!
Ao me inscrever, aceito plenamente todos os [Termos e Condições](#) do programa
[Saiba mais sobre o nosso programa de fidelidade](#)

- ☒ Desejo receber por e-mail promoções, ofertas de última hora e informações sobre hotéis
- ☐ Continuar conectado (em caso de computador compartilhado, desmarque esta opção)
- ☐ Li e aceito os [Termos e condições](#) e a [política de privacidade](#) deste site

[Criar sua conta](#)

Site de Compras

Pessoa Física

☒ Pessoa Física ☐ Pessoa Jurídica

*Como gostaria de ser chamado?

*Nome completo

*CPF

*Data de Nascimento

*Sexo

Selecione ▾

*Telefone Principal

 -

(DDD - TELEFONE)

Telefone Celular

 -

(DDD - TELEFONE) (OPCIONAL)

Telefone Comercial

 -

(DDD - TELEFONE - RAMAL) (OPCIONAL)

Primeiro digite o CEP:

01501

050

OK

Não sabe o CEP, [consulte Aqui](#)

*Identificação do Endereço

☐ Apartamento ☒ Casa ☐ Comercial ☐ Outro (Ex: Casa dos pais, Casa de praia, etc.)

*Endereço

Sete de Setembro

*Número

Complemento

Ex: Apto 203

*Bairro

Centro

*Cidade

São Paulo

*Estado

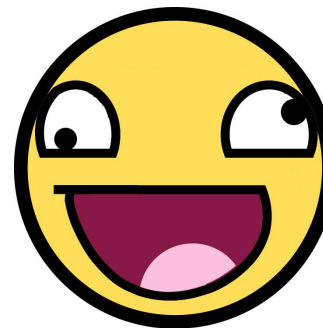
SP

*País

BR

Informações de referência

Atenção: não fazemos entregas em endereço de caixa postal





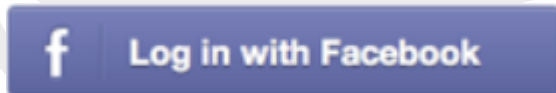
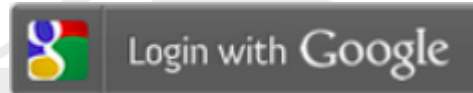
Resultado Final

MUITO TRABALHO!

Identidade

- Unicidade de um indivíduo
- Histórico
- "Identidade Virtual"
- Identity 1.0

Mas, e se...



Histórico

OpenID (Yadis)

OpenID 2.0

OpenID Foundation

OpenID Connect

OpenID Connect

- O que é ?
- OAuth 2.0
- Identity 2.0

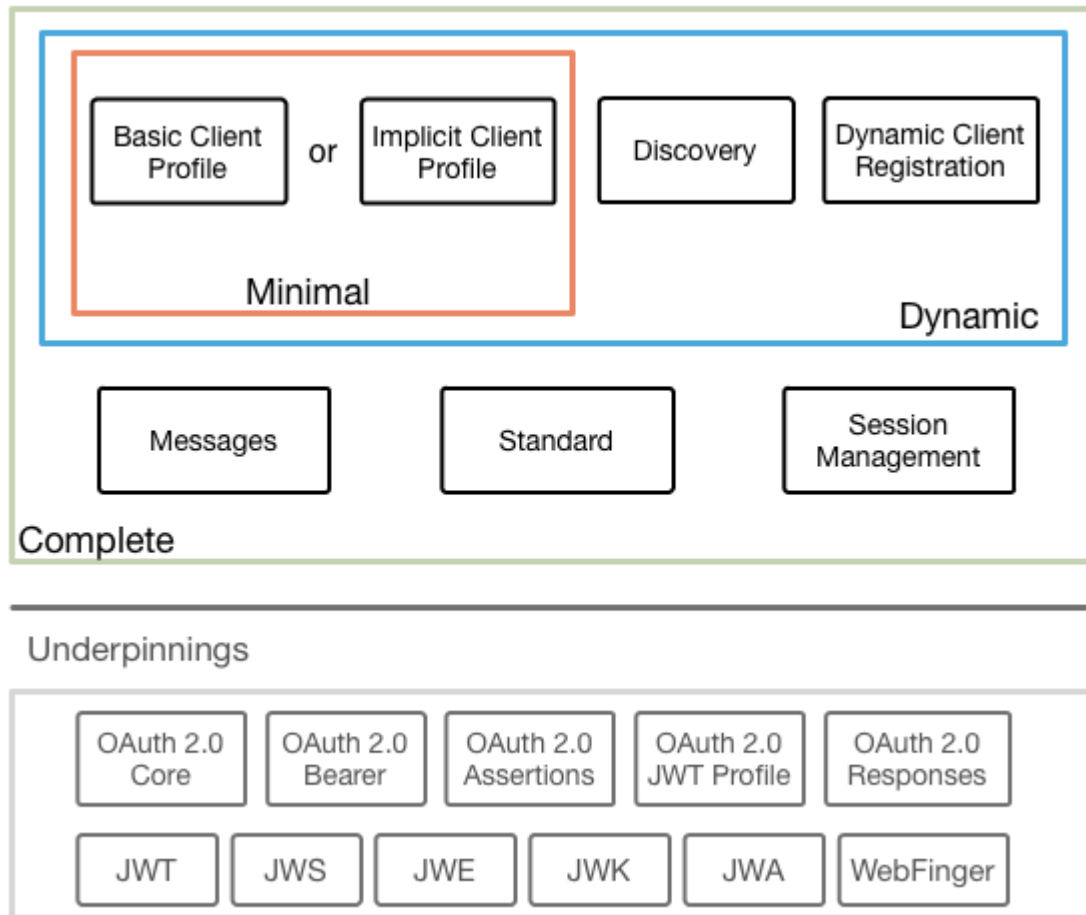
OpenID Connect

- Autenticação
- Autorização

OpenID x OpenID Connect

- API amigável
- OAuth 2.0 integrado
- Facilidade para dispositivos móveis
- Especificações modulares

Organização das Especificações



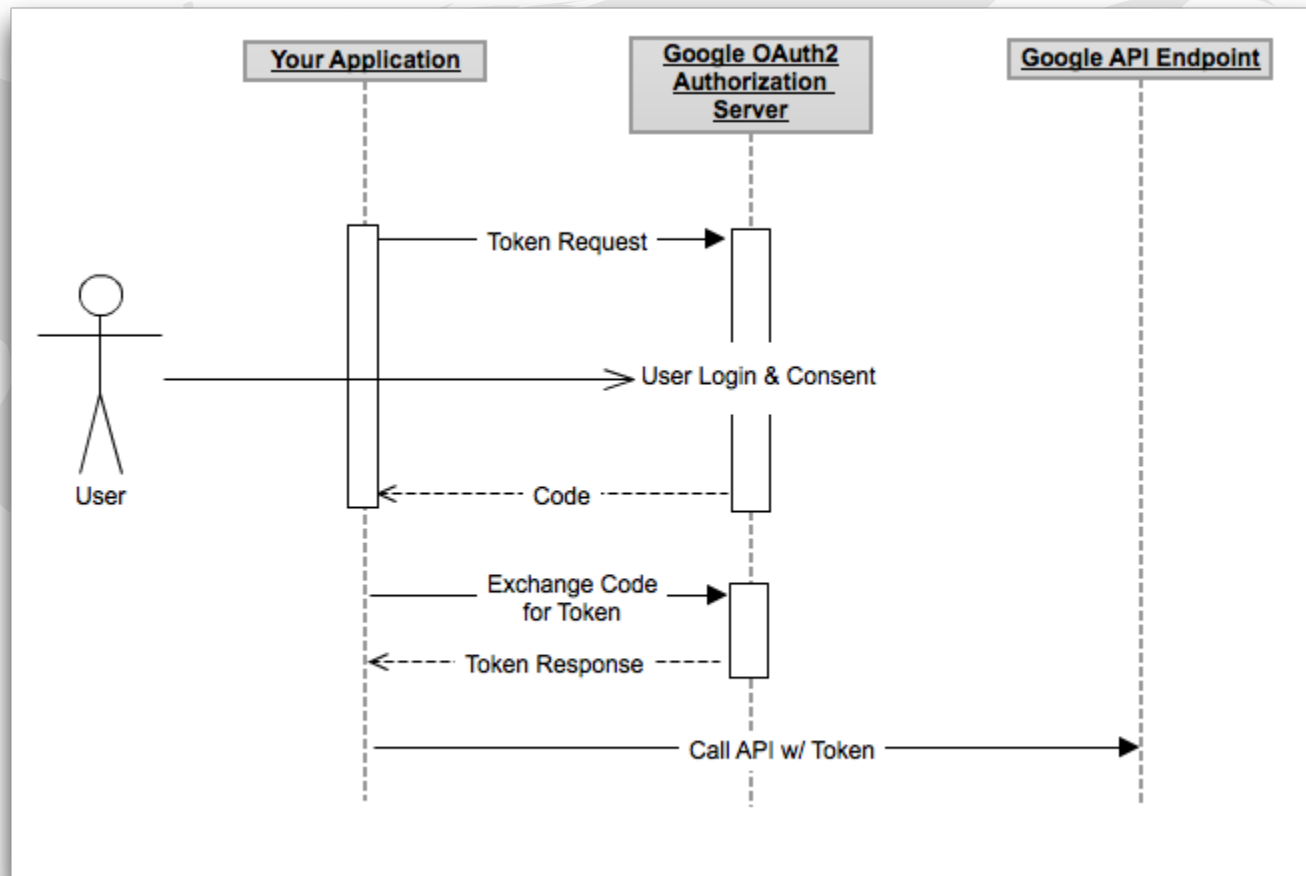
Organização das Especificações

- Composto por 8 documentos:
 - Basic Client Profile
 - Implicit Client Profile
 - Discovery (Opcional)
 - Dynamic Registration (Opcional)

Organização das Especificações

- Composto por 8 documentos:
 - Messages
 - Standards
 - Session Management (Opcional)
 - OAuth 2.0 Multiple Response Types

OpenID Connect Google



Solicitação OpenID Connect

São necessários algumas informações para que o cliente faça uma requisição OpenID Connect:

- Client Id
- Client Secret
- Authorization Endpoint

Solicitação OpenID Connect

- Token Endpoint (usuário)
- UserInfo Endpoint
- Check Id Endpoint (Foi revogado em 2012)

Exemplo GitHub

- Um usuário do GitHub deseja se autenticar em uma aplicação utilizando sua conta do GitHub.
- A aplicação no qual o usuário se autenticou deseja utilizar uma funcionalidade do GitHub.

Exemplo GitHub

- O usuário deverá provar quem ele é.
- A aplicação pede permissão para o usuário para obter infos do GitHub.
- O GitHub é quem intermediará o acordo entre o usuário e a aplicação.

Exemplo GitHub

GET:

`http://localhost:7000/autenticacao`

Aplicação

Usuário

1

```
graph LR; User[Usuário] --> Application[Aplicação];
```

The diagram illustrates a request flow. A green box labeled 'Usuário' (User) is on the right, and a red box labeled 'Aplicação' (Application) is on the left. A horizontal arrow points from the User box to the Application box. Below this arrow, centered, is a dark brown circle containing the white number '1', indicating the first step in the process.

Exemplo GitHub

HTTP 303:

[https://github.com/login/oauth/authorize?
client_id=86e455857d5e2b2464c0&redirect_url=h
ttp://localhost:
7000/autenticacao/retorno&scope=user:email](https://github.com/login/oauth/authorize?client_id=86e455857d5e2b2464c0&redirect_url=http://localhost:7000/autenticacao/retorno&scope=user:email)

Aplicação

Usuário

2

Exemplo GitHub

GET:

`https://github.com/login/oauth/authorize?
client_id=86e455857d5e2b2464c0&redirect_url=h
ttp://localhost:
7000/autenticacao/retorno&scope=user:email`

Usuário

GitHub

3

Exemplo GitHub

HTTP 302:

```
https://github.com/login?return_to=https://github.com/login/oauth/authorize?client_id=86e455857d5e2b2464c0&redirect_url=http://localhost:7000/autenticacao/retorno&scope=user:email
```

Usuário

GitHub

4

Exemplo GitHub

GET:

```
https://github.com/login?return_to=https://github.com/login/oauth/authorize?client_id=86e455857d5e2b2464c0&redirect_url=http://localhost:7000/autenticacao/retorno&scope=user:email
```

Usuário

GitHub

5

Exemplo GitHub

HTTP 200:

```
https://github.com/login?return_to=https://github.com/login/oauth/authorize?client_id=86e455857d5e2b2464c0&redirect_url=http://localhost:7000/autenticacao/retorno&scope=user:email
```

Usuário

GitHub

6

Exemplo GitHub

POST:

```
https://github.com/login?return_to=https://github.com/login/oauth/authorize?client_id=86e455857d5e2b2464c0&redirect_url=http://localhost:7000/autenticacao/retorno&scope=user:email
```

Usuário

GitHub

7

Exemplo GitHub

HTTP 302:

`https://github.com/login/oauth/authorize?
client_id=86e455857d5e2b2464c0&redirect_url=h
ttp://localhost:
7000/autenticacao/retorno&scope=user:email`

Usuário

GitHub

8

Exemplo GitHub

GET:

`https://github.com/login/oauth/authorize?
client_id=86e455857d5e2b2464c0&redirect_url=h
ttp://localhost:
7000/autenticacao/retorno&scope=user:email`

Usuário

GitHub

9

Exemplo GitHub

HTTP 200:

`https://github.com/login/oauth/authorize?
client_id=86e455857d5e2b2464c0&redirect_url=h
ttp://localhost:
7000/autenticacao/retorno&scope=user:email`

Usuário

GitHub

10

Exemplo GitHub

POST:

```
https://github.com/login/oauth/authorize?  
client_id=86e455857d5e2b2464c0&redirect_url=h  
ttp://localhost:  
7000/autenticacao/retorno&scope=user:email
```

Usuário

GitHub

11

Exemplo GitHub

HTTP 302:

**`http://localhost:
7000/autenticacao/retorno&code=67847d419a1fad
3e8021`**

Usuário

GitHub

12

Exemplo GitHub

GET:

**`http://localhost:
7000/autenticacao/retorno&code=67847d419a1fad
3e8021`**

Aplicação

Usuário

13

Exemplo GitHub

POST:

`https://github.com/login/oauth/access_token?
client_id=86e455857d5e2b2464c0?
client_secret=31a5bc760219bf2b8dcb0539fa20981
eeb3c7479?code=67847d419a1fad3e8021`

Aplicação

GitHub

14

Exemplo GitHub

HTTP 200:

```
{"token_type": "bearer", "access_token":  
"b6c27ff7c1a0fa1ece61c3ecef2ba62d2c37a43f"}
```

Aplicação

GitHub

15

Exemplo GitHub

GET:

`https://api.github.com/user/emails?
access_token=b6c27ff7c1a0fa1ece61c3ecef2ba62d
2c37a43f`

Aplicação

GitHub

16

Exemplo GitHub

HTTP 200:

```
["lucaspereira@inf.ufsc.br",  
 "pslucasps@gmail.com"]
```

Aplicação

GitHub

17

Exemplo GitHub

HTTP 200:

```
{"emailsDoUsuario": ["lucaspereira@inf.ufsc.br", "pslucasps@gmail.com"], "tokenDeAcesso": {"token_type": "bearer", "access_token": "b6c27ff7c1a0fa1ece61c3ecef2ba62d2c37a43f"}}
```

Aplicação

Usuário

18