Guia rápido de utilização do OAuth2 do FA

Conteúdo

Palavras chave:

- FA – Fornecedor de Atributos;
- CMD – Chave Móvel Digital

O FA utiliza a autenticação *Implicit Grant* do OAuth2 para fazer a autenticação e devolver os atributos pedidos em dois passos, primeiro é necessário obter um *token* e de seguida é necessário fazer um pedido com esse token de forma a obter os atributos associados.

Fluxo de obtenção do token

1. Primeiro é feito um pedido ao site do FA com os seguintes parâmetros de entrada:

- `response_type` com o valor `token`;
- `client_id` com o identificador do sistema requerente, acordado previamente;
- `redirect_uri` com o *url* de redireccionamento, para voltar para o sistema requerente. Este parâmetro é opcional e caso não seja enviado será devolvido para uma página estática do FA. Caso seja utilizado o *host* desse url deve ser previamente acordado;

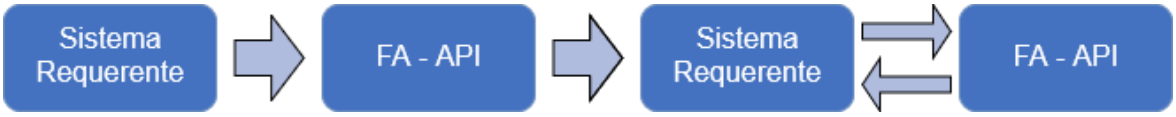
  url de exemplo com o *host* destacado:
  - http://127.0.0.1:8000/examplePath
- `scope` uma lista de atributos delimitada com um espaço entre cada um. É obrigatório incluir o atributo http://interop.gov.pt/MDC/Cidadao/NIC para cidadãos portugueses ou os atributos http://interop.gov.pt/MDC/Cidadao/DocNumber,

http://interop.gov.pt/MDC/Cidadao/DocNationality e http://interop.gov.pt/MDC/Cidadao/DocType para os cidadãos estrangeiros;
- `authentication_level` - Nível de segurança da operação, este parâmetro define as opções de autenticação disponíveis, por omissão este valor é 3. (ver Anexo A)
- `default_selected_tab` - Opção de autenticação escolhida por omissão. Se a opção aqui especificada entra em conflito com as opções escondidas, ambos os parâmetros são ignorados.
- `hidden_tabs` - Opções de autenticação escondidas ao utilizador. Se todas as opções possíveis forem escondidas este parâmetro é ignorado.
- `state` – Parametro de segurança do OAuth. Quando preenchido, as respostas do servidor vão conter este mesmo state no URL (num parâmetro do redirect_uri) para que o cliente possa ter a certeza de que a resposta que obteve foi a resposta a um pedido realizado por si. Se o *state* que vem na resposta do servidor for diferente do enviado pelo cliente, este deve ignorar esta resposta e realizar novo pedido. (Este parâmetro é opcional)

2. De seguida é pedido ao utilizador que autorize a leitura dos atributos por parte do sistema requerente.
3. O utilizador irá ser redirecionado para a CMD de forma a autenticar-se com as suas credenciais.
4. Assim que é validada a autenticação com sucesso, o cliente é redirecionado para o *url* inserido no parâmetro *`redirect_uri`* anteriormente e são devolvidos ao sistema requerente os seguintes parâmetros na *query string*:

- `token_type` com o valor `Bearer`;
- `expires_in` com um *long* representando o tempo de vida do *access token*;
- `access_token` o *token* gerado pelo FA para se utilizar no segundo passo de obtenção dos atributos;
- `state` com o mesmo valor inserido no pedido inicial

Fluxo de obtenção dos atributos



- O sistema requerente após obtenção do *access token* no fluxo anterior, envia este access token para a API do FA através de um método POST passando um objecto JSON do tipo:

- `token` com o valor do *token* obtido no passo anterior;
- `attributesName` com um uma *lista de strings* dos atributos a filtrar. Este parâmetro é opcional e caso não seja preenchido irá retornar todos os atributos relacionados com o *token*.

- A API do FA retorna um objecto JSON com os seguintes atributos:

- `token` com o valor do *token* obtido no passo anterior;
- `authenticationContextId` – Identificador do processo de autenticação.

- O sistema requerente deve depois utilizar esses atributos como parâmetros num pedido GET para obter os valores dos atributos pedidos.

  Formato do pedido GET:
  <FA-API URL>?token=<token>&authenticationContextId=<authenticationContextId>

- Após o FA validar o token com sucesso é devolvida a lista em JSON com os valores desses atributos que já tenham sido obtidos, os atributos que ainda não tenham sido obtidos são devolvidos com o valor *null*. (Ver nota abaixo)

NOTA IMPORTANTE: Como a obtenção de atributos poderá demorar algum tempo dependendo dos atributos pedidos e de sistemas externos, os atributos pedidos poderão não estar disponíveis na altura em que é feito o pedido ao sistema FA. Cabe ao sistema requerente decidir como agir nestas situações. A única restrição é que não seja efetuado mais que um pedido por segundo à API do FA.

URLs

- FA – OAuth
  - Pedido de entrada: https://preprod.autenticacao.gov.pt/OAuth/AskAuthorization
  - Página estática de retorno: https://preprod.autenticacao.gov.pt/OAuth/Authorized
- FA – API
  - https://preprod.autenticacao.gov.pt/OAuthResourceServer/Api/AttributeManager

Possíveis erros

Os erros virão na forma de (caso seja para o endereço estático do FA)
https://preprod.autenticacao.gov.pt/oauth/authorized#error=XXXXX

- `invalid_request` – quando é um pedido inválido por exemplo com campos obrigatórios vazios
- `unauthorized_client` – quando o id do cliente é inválido
- `unsupported_grant_type` – quando o *grant_type* passado não equivale a *token*
- `cancelled` – quando o utilizador cancela o login

No caso da API, virão em JSON.

Exemplo prático

1. Envio de um pedido para o site https://preprod.autenticacao.gov.pt/oauth/askauthorization?redirect_uri=https://preprod.autenticacao.gov.pt/OAuth/Authorized&client_id=123456789&scope=http://interop.gov.pt/MDC/Cidadao/NomeProprio%20http://interop.gov.pt/MDC/Cidadao/NIC%20http://interop.gov.pt/MDC/Cidadao/DataNascimento%20http://interop.gov.pt/MDC/Cidadao/NIF&response_type=token

2. Após autorização é redirecionado para o site da CMD

3. É feita a autenticação e inserido o pin

4. É retornado para a página estática, que deverá ser intercetada pelo sistema requerente e que o url é https://preprod.autenticacao.gov.pt/oauth/authorized#access_token=11dd26e4-a1f4-4626-8834-001c00b9158c&token_type=bearer&expires_in=86400
5. Depois deverá ser enviado um pedido para a API na forma de https://preprod.autenticacao.gov.pt/oauthresourceserver/api/AttributeManager com o body preenchido com o token e possíveis atributos:
   `{"token": "0e3e71b6-5ce5-462d-bb1c-b27b83c51e1f","attributesName":["http://interop.gov.pt/MDC/Cidadao/FotoCVCCD","http://interop.gov.pt/MDC/Cidadao/NIF"]}`
6. Obtendo assim o resultado em JSON
   {"token": "a7ff26fb-392e-433b-94d6-c7182b5e7983",
   "authenticationContextId": "b3e98d70-dc69-4e5b-bafa-184da35c0a13"}
7. Depois deverá ser enviado um pedido GET para a API na forma:
   https://preprod.autenticacao.gov.pt/oauthresourceserver/api/AttributeManager?token=a7ff26fb-392e-134b-94d6-c7182b5e7983&authenticationContextId= b3e98d70-dc69-4e5b-bafa-1849a35c1233
8. Obtendo como resultado em JSON:
   [{"name": "http://interop.gov.pt/MDC/Cidadao/FotoCVCCD","value": null},
   {"name": "http://interop.gov.pt/MDC/Cidadao/NIF","value": "258476745"}]
9. Como os atributos não foram todos devolvidos o sistema repete o mesmo pedido de 2 em 2 segundos até receber todos os atributos ou passarem 30 segundos ao que assume que o atributo pedido não se encontra disponível.

Anexos

A

Nível de Autorização	Descrição	Opções de Autenticação
4	Elevado – Permite acesso a todos os atributos de um cidadão	Apenas com acesso presencial ao Cartao de Cidadão
3		