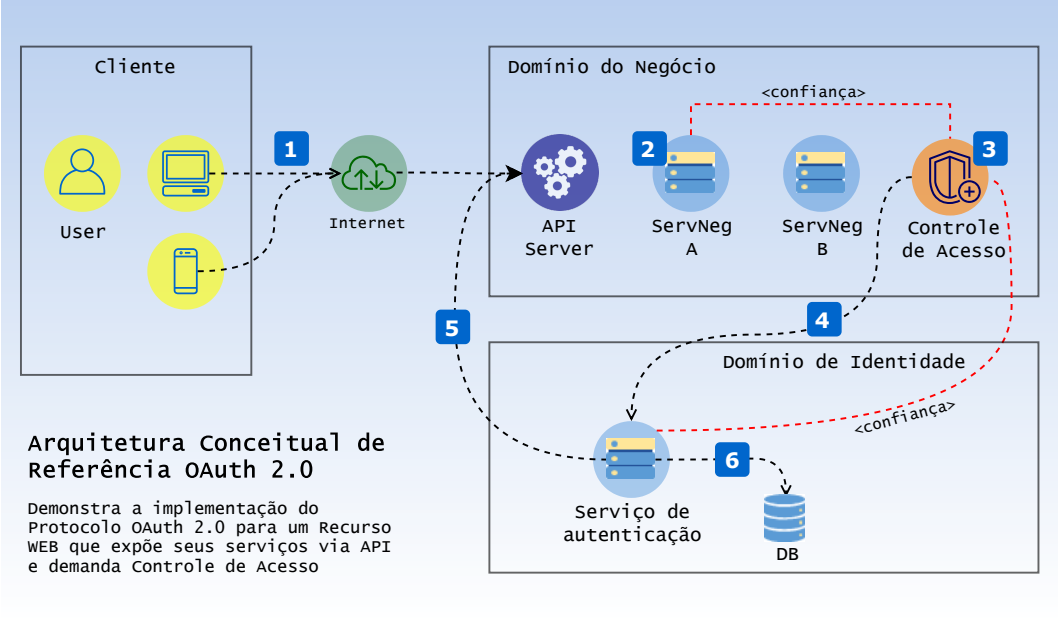

#interna

1 O usuário requisita o recurso (serviço de Negócio).

2 O recurso recebe a solicitação e aciona o Controle de Acesso para resolver as questões de segurança

3 O Controle de Acesso recebe a requisição do Serviço de Negócio para verificar as regras de segurança. Conforme abaixo, se:

(A) 1o Acesso - Usuário deve fazer Login
(B) Conferência de Token - conforme regra de validade do Token de Acesso

(A) 1o Acesso - Usuário deve fazer Login

O Controle de Acesso aciona a API de Autenticação que apresenta a tela de Login ao Usuário.

O Cliente informa suas credencias de acesso (ID/Senha).

4 O Controle de Acesso entrega a API de Autenticação ao Serviço de Autenticação para a validação das credenciais.

O Serviço de Autenticação confere os dados, uma vez válidos, emite o Token de Acesso + Token de Atualização e devolve ao Controle de Acesso.

RECURSO LIBERADO AO USUÁRIO

O Controle de Acesso autoriza o Serviço de Negócio a liberar o acesso ao usuário ao Recurso e entrega o Token de Acesso + Token de Atualização para o Serviço de Negócio. (Uma vez que o Serviço de Negócio recebe o Token de Acesso + Token de Atualização o usuário passa a acessar o recurso.)

(B) Conferência de Token - conforme regra de validade do Token de Acesso

O usuário solicita acesso a um Recurso do Serviço de Negócio.

O Serviço de Negócio de posse do Token de Acesso + Token de Atualização entrega ao Controle de Acesso para verificar se ainda encontra-se válido.

4 O Controle de Acesso verifica se é o caso de solicitar novo Token de Acesso (nesse caso revoga o Token e solicita novo Login ao usuário) ou solicita ao Serviço de Autenticação que revalide o Token de Acesso com base no Token de Atualização.

O Controle de Acesso recebe o Token de Acesso revalidado e autoriza o Serviço de Negócio a liberar o acesso ao usuário ao Recurso e entrega o Token de Acesso + Token de Atualização para o Serviço de Negócio. (Uma vez que o Serviço de Negócio recebe o Token de Acesso + Token de Atualização o usuário passa a acessar o recurso.)

5 O Serviço de Autenticação expõe API de Autenticação para fins do Serviço de Autenticação a ser consumido pelos Serviços de Negócio de que demandam Controle de Acesso.

6 BD - Repositório de Indentidade e Credenciais de Acesso gerenciado e acessado pelo Serviço de Autenticação

REQUISITOS DA SOLUÇÃO

RA. O serviço de Negócio A não é de acesso público requer Controle de Acesso ao recurso.

RB. O serviço de Negócio que requeira controle de acesso fará uso do Serviço de Autenticação (LOGIN).

RG. O Serviço de Negócio expõe seus recursos(serviços) por meio de APIs.

RH. O Serviço de Negócio confia no Controle de Acesso para resolver as regras de segurança (Identificação, Autenticação e Autorização)

RJ. O Serviço de Negócio não implementa o Serviço de Autenticação. Faz uso de Serviço de Autenticação por meio de API de Autenticação disponibilizada pelo Serviço de Autenticação.

RI. Deve ser estabelecido a confiança entre o Controle de Acesso e o Serviço de Negócio assim como entre o Controle de Acesso e o Serviço de Autenticação

RI. O Controle de Acesso conhece a API de Autenticação disponibilizada pelo Serviço de Autenticação

RC. O elemento de segurança que habilita o acesso ao recurso é o Token de Acesso e respectivo Token de Atualização.

RD. O Token de Acesso deve ter prazo de expiração podendo ser revogado a qualquer momento.

RE. O prazo de validade do Token de Acesso pode ser revalidado com base no Token de Atualização.

RF. O Token de Atualização é opcional porém se for emitido esté estará vinculado ao Token de Acesso e deve ter política de uso. (Ex.: número de vezes que pode ser usado para revalidar um Token de Acesso)

Na Arquitetura apresentada	Protocolo OAuth 2.0
Aplicação Cliente	API do Negócio
Serviço de Autenticação	Authentication Server
Serviço de Negócio	Resource Owner
Token de Acesso	Acess Token
Token de Atualização	Refresh Token

Responsável pela Arquitetura
F2191149-5 Cristina R. Souza
Atualizada em 04/2020

FLUXO DE AUTORIZAÇÃO DE ACESSO A RECURSOS USANDO OAUTH 2.0 (RFC 6749, 4.1

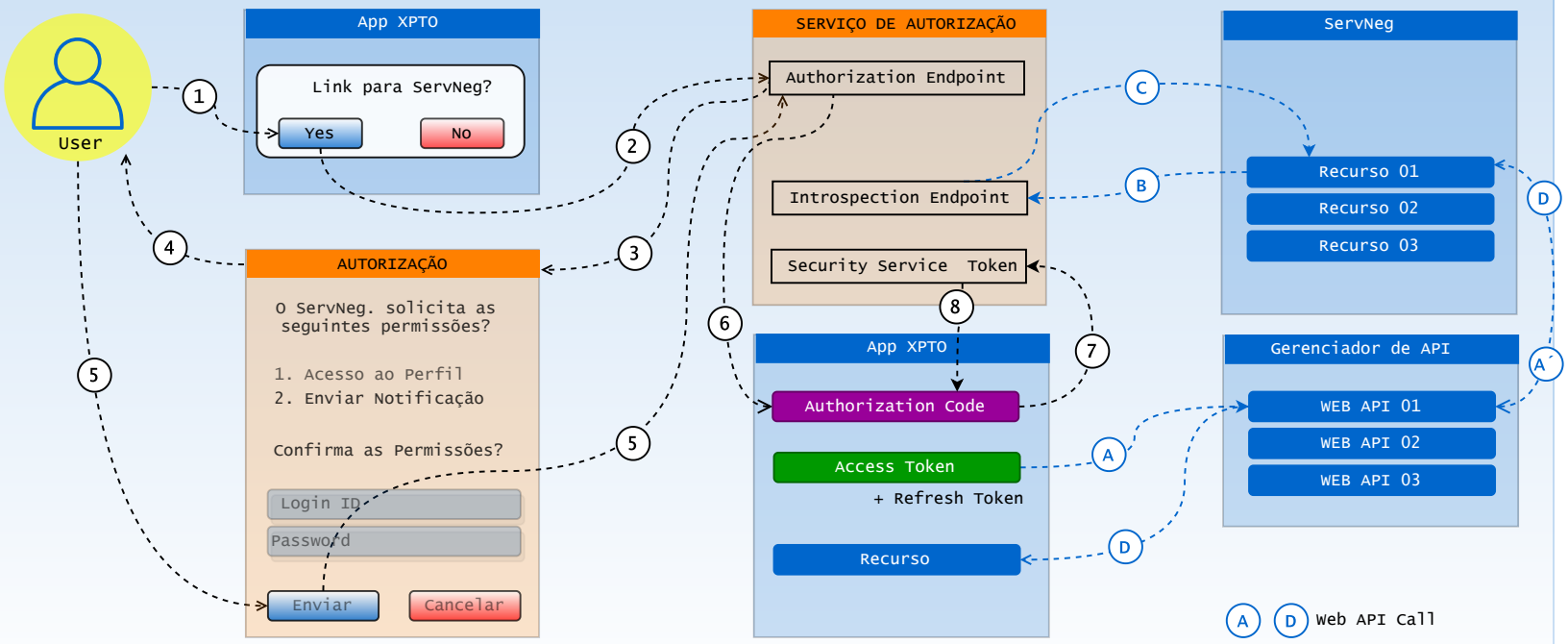

FIG. 01

1 O usuário deseja acesso ao serviço de negócio (recurso x) e clica no LInk que vincula o App XPTO (Cliente) ao ServNeg.

2 O App faz a requisição ao Serviço de Autorização.(Authorization Request)

3 O Serviço de Autorização retorna uma página ao App XPTO para colher a autorização do usuário. (Authorization Page)

4 O App XPTO apresenta a página de autorização ao usuário.

5 O usuário deve verificar quais as permissões requeridas pelo ServNeg. e informar seu ID/Senha de Login e confirmar (enviar) a requisição de autorização.

Se o usuário entender que não quer dar as permissões pedidas pode cancelar a requisição porém não obterá acesso ao recurso desejado.

6 O Serviço de Autorização emite um código de autorização de curta duração. (Authorization Code) e entrega ao App XPTO.

7 O App XPTO apresenta o código de autorização curta ao SST (Service Security Token). (Service Token Endpoint)

8 O Serviço de Autorização emite o Token de Acesso e entrega ao App XPTO.(Access Token)

A O App XPTO apresenta o Token de Acesso e requisita o acesso ao recurso.

A' Post ao recurso repassando o Token de Acesso

B O ServNeg apresenta o Token de Acesso ao Serviço de Autorização e requisita a validação do mesmo.

C O Serviço de Autorização confirma ou não a validade do Token de Acesso.

D O ServNeg verifica a resposta do Serviço de Autorização, se "OK", libera o acesso ao recurso ao App XPTOconfirma ou não a validade do Token de Acesso.

4.1 The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. Since this is a redirection-based flow, the client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.

4.1 O código concessão de autorização é um elemento usado para obter os dois tokens de acesso Token de Acesso e Token de Atualização (Access Token e Refresh Token) é otimizado para clientes confidenciais. Como esse é um fluxo baseado em redirecionamento, o cliente deve ser capaz de interagindo com o user-agent do proprietário do recurso (geralmente um navegador) e capaz de receber solicitações de entrada (via redirecionamento) do servidor de autorização.

Referências:

https://medium.com/@darutk/new-architecture-of-oauth-2-0-and-openid-connect-implementation-18f408f9338d

https://www.tutorialspoint.com/oauth2.0/index.htm

https://tools.ietf.org/html/rfc8252

https://tools.ietf.org/html/rfc6749 (atualiza pela RFC 8252)

https://oauth.net/2/

1.5 Access Token

Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. The string is usually opaque to the client. Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorization server.

Os tokens de acesso são credenciais (elementos de segurança) usadas para acessar recursos protegidos. Um token de acesso é uma cadeia que representa uma autorização emitida para o cliente. Representado por um String é opaco ao Cliente e representam escopos e durações específicas de acesso, concedidos pelo proprietário do recurso e imposta pelo servidor de recursos e acatada pelo seridor de autorização. (Regras de Negócio traduzidas em Requisitos de Segurança para acesso ao Serviço)

1.5 Refresh Token

Refresh tokens are credentials used to obtain access tokens. Refresh tokens are issued to the client by the authorization server and are used to obtain a new access token when the current access token becomes invalid or expires, or to obtain additional access tokens with identical or narrower scope (access tokens may have a shorter lifetime and fewer permissions than authorized by the resource owner). Issuing a refresh token is optional at the discretion of the authorization server. If the authorization server issues a refresh token, it is included when issuing an access token (i.e., step (D) in Figure 1).

Os tokens de atualização são credenciais usadas para obter tokens de acesso. Tokens de Atualizações são emitidos para o cliente pelo servidor de autorização e são usados para obter um Novo Token de Acesso quando o Token de Acesso Atual torna-se inválido ou expira ou para obter Tokens de Acesso Adicionais com escopo idêntico ou menores (os tokens de acesso devem ter vida útil e menos permissões do que as autorizadas pelo recurso proprietário). A emissão de um token de atualização é opcional, a critério do servidor de autorização (regra de segurança para o serv. de negócio). Se o servidor de autorização emitir um tokende atualização este virá acoplado ao token de acesso requerido.

Cristina R. Souza - Edição e Tradução com ajustes