OIDC

Use uma identidade verificada para iniciar a sessão

Pré-requisitos

Conheça HTTPS, redirecionamento e a diferença entre navegador, aplicação e API. O exercício assume um portal que usa um provedor de identidade (OP) para autenticar clientes. O portal é o cliente OIDC, também chamado de relying party.

Separe autenticação e acesso [1]

OIDC acrescenta uma camada de identidade ao OAuth 2.0. O escopo openid indica um pedido OIDC. O ID token contém declarações sobre a autenticação e é destinado ao cliente. Um access token serve para acessar o recurso para o qual foi concedido. A API de agendamentos ainda precisa aplicar sua própria política para decidir quem pode consultar ou cancelar uma reserva.

Entenda o fluxo com código [1][3]

O portal inicia a autenticação redirecionando o navegador ao provedor. Depois da autenticação, o navegador volta ao endereço de retorno cadastrado com um código. O portal troca o código no endpoint de token da configuração confiável. PKCE com S256 vincula a troca ao verificador mantido pelo cliente para aquela tentativa. Faça a integração com uma biblioteca OIDC mantida e use HTTPS em produção.

Dê uma função a cada vínculo

Use state para correlacionar o retorno com a tentativa iniciada no navegador. Se a aplicação enviou nonce, a biblioteca deve comparar o valor do ID token com o da tentativa. Mantenha state, nonce e o verificador PKCE associados à tentativa e expire-os. Depois de validar a identidade, o portal pode criar uma sessão própria e usar as permissões do usuário para proteger as operações.

Configure o emissor a partir de dados confiáveis [2]

Use o endereço de emissor configurado para obter os metadados. Confira se o issuer retornado tem o valor esperado. Os metadados informam endpoints de autorização, token e JWKS. Use as chaves e algoritmos permitidos na integração para verificar a autenticidade do ID token. A aplicação precisa tratar rotação de chaves sem aceitar chaves de origens arbitrárias.

OIDC

Exercício resolvido • Revise uma integração

Enunciado e dados de partida

O portal de agendamentos tem client_id agenda-web. O emissor esperado é https://identidade.example e o retorno cadastrado é https://agenda.example/oidc/retorno. O pedido usa Authorization Code, PKCE S256, scope openid e um nonce. Na tentativa fictícia, o state esperado é S7 e o nonce é N7. Use o instante de referência 12h00 UTC, com tolerância de relógio zero neste exercício.

1. Resolva o retorno normal

O portal recebe o código e state S7 em seu endereço de retorno. Associe-os à tentativa iniciada, troque o código com o verificador PKCE e valide o ID token via biblioteca. O token do cenário tem assinatura válida, issuer esperado, audiência agenda-web, nonce N7, expiração às 12h05 UTC e subject p-540. A expiração está cinco minutos no futuro. As checagens apresentadas passam.

2. Defina a identidade gravada

Associe a conta local ao par (https://identidade.example, p-540). Um subject identifica a pessoa no escopo do emissor. O e-mail pode mudar e pode servir para contato conforme o contrato de perfil escolhido. Só depois de resolver a conta local crie a sessão de navegação. O papel de cliente ou recepção vem da política de acesso do sistema.

3. Revise os dados que saem do portal

No redirecionamento de autorização, a aplicação inclui a URI de retorno registrada e o desafio PKCE. Na troca, fornece o verificador e, quando o cliente é confidencial, usa o mecanismo de autenticação cadastrado. A aplicação evita registrar códigos, tokens e verificadores. Ao registrar um erro, preserve etapa e motivo suficientes para a equipe identificar a configuração afetada.

OIDC

Confira as condições que bloqueiam a sessão

Caso de erro • Retorno sem correlação

Se a tentativa esperava S7 e o retorno traz outro valor, encerre o fluxo antes da troca do código. O portal pode oferecer reiniciar o login. Registre o motivo de maneira genérica e mantenha os valores da tentativa fora da mensagem ao usuário.

Variações de validação do token

Mantenha os demais dados do cenário e altere um item por vez: audiência agenda-admin, nonce diferente ou expiração às 11h59 UTC. Cada variação impede a criação da sessão. Se houver mais de uma audiência, avalie também as regras de parte autorizada aplicáveis ao cliente, conforme a especificação e a biblioteca. Uma assinatura válida sozinha é insuficiente.

Critérios para conferir a resposta

O caso normal leva a uma única sessão associada ao par emissor e subject. Um retorno sem correlação não chega ao endpoint de token. Em cada variação de token, a sessão permanece ausente. Verifique também que uma sessão autenticada do cliente não concede acesso aos agendamentos de outra pessoa.

Como usar o exercício

As URLs .example e os valores curtos são material ilustrativo para revisão em papel, sem provedor ativo. Em homologação, configure um cliente próprio no provedor e use os testes da biblioteca para checar o fluxo com metadados, chaves, relógio e usuários de teste. Não trate a revisão em papel como validação da integração em produção.

Referências primárias

[1] OpenID Foundation • OIDC Core, Authorization Code Flow

[2] OpenID Foundation • Discovery, metadados do provedor

[3] IETF • RFC 9700, Authorization Code e PKCE

OIDC

Separe a sessão web do acesso à API

Defina o destinatário de cada token

O aplicativo usa o ID token validado para reconhecer o login. Uma API que recebe access tokens deve verificar se o token é destinado a ela e se permite a ação solicitada.

Exercício adicional

O login funciona, mas a API recebeu um token destinado a outro serviço. Qual é o comportamento esperado?

Resolução

Rejeite o token na API e obtenha um access token destinado à agenda. Use a biblioteca de validação do provedor e teste a audiência esperada e a rejeição de uma audiência diferente.

Ao assistir ao vídeo

Identifique quem consome o ID token e quem recebe o access token.

Vídeo complementar

Entenda de vez OAuth 2.0 e OpenID Connect