JWT

JSON WEB TOKENS

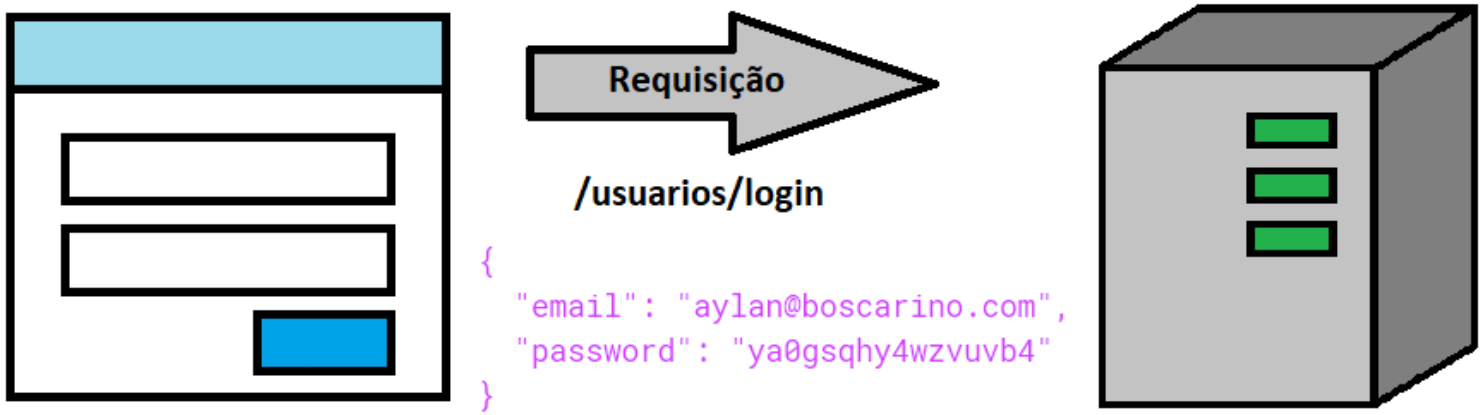
www.cotiinformatica.com.br

JWT – JSON WEB TOKENS

o **JWT (JSON Web Token)** é um sistema de transferência de dados que pode ser enviado via POST ou em um cabeçalho HTTP (header) de maneira “segura”, essa informação é assinada digitalmente por um algoritmo HMAC, ou um par de chaves pública/privada usando RSA. Podemos ver na imagem a baixo um cenário onde será requisitado um token através do Verbo HTTP POST, que irá devolver um token validado para que nas próximas requisições que utilizem os Verbos HTTP possam utilizar.

A assinatura de um JSON Web Token é seu componente mais sensível por tratar justamente da segurança deste token. Por conta disto existe uma fórmula padrão para que o token seja adequadamente assinado, exigindo que o token seja uma hash em Base64 gerada de um algoritmo de criptografia, por exemplo SHA256 ou SHA512, e essa hash precisa ser feita a partir do header e do payload do token.

JWT – JSON WEB TOKENS

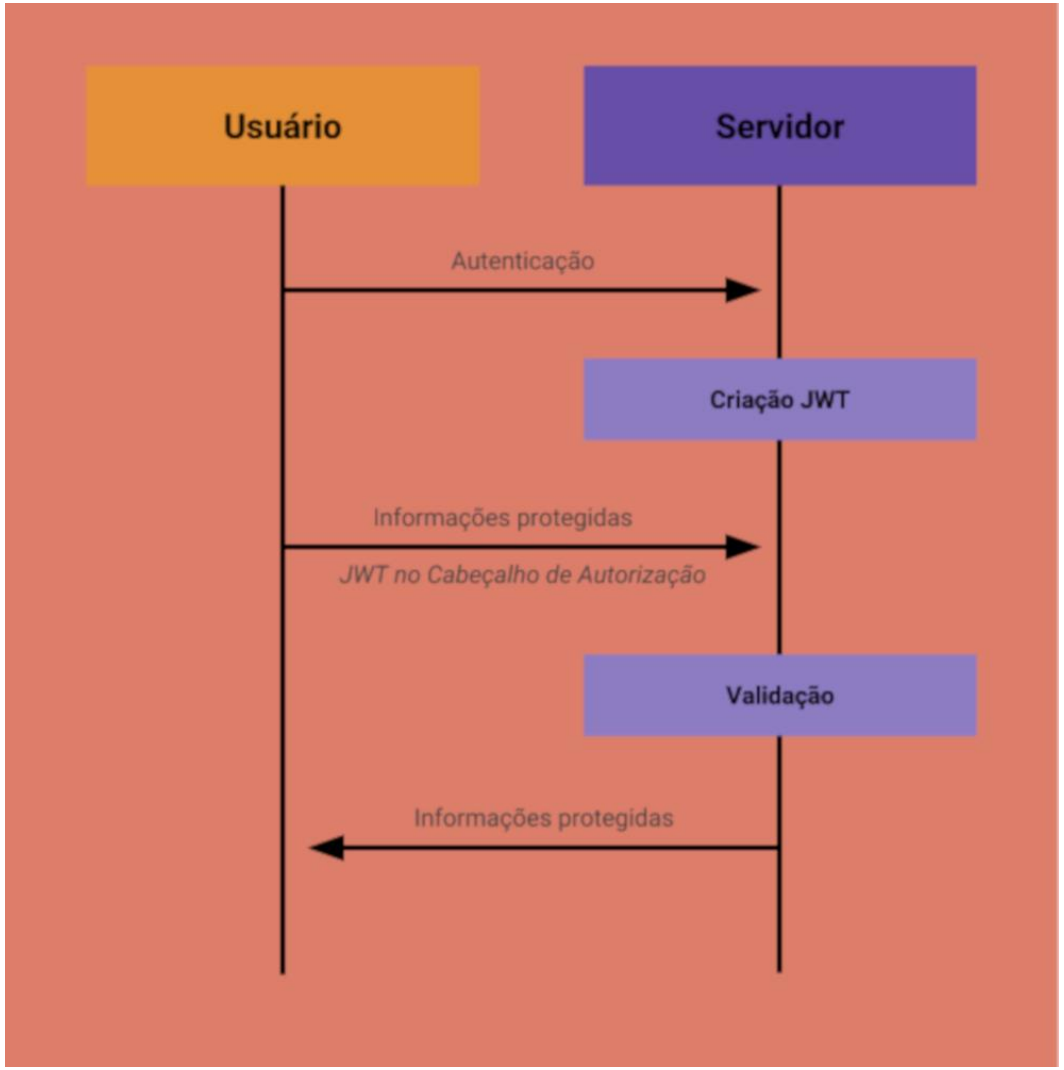


JWT – JSON WEB TOKENS

O JWT é útil em diversos cenários, porém os dois mais comuns são:

Autenticação: O token é utilizado para verificar a identidade de um usuário e suas permissões. Esses tokens normalmente incluem identificadores e informações não sensíveis do usuário.

Troca de informação: Por ser um meio seguro para duas aplicações conversarem, graças a maneira que os tokens são assinados digitalmente, eles garantem a identidade das partes envolvidas e se a informação não foi alterada no meio da caminho.



JWT – JSON WEB TOKENS

1. O usuário envia as informações necessárias para autenticação.
2. O servidor valida as informações, gera e retorna o JWT para o usuário.
3. Com o JWT em mãos, o usuário agora pode realizar requisições autenticadas enviando o cabeçalho de autorização: Authorization: Bearer <token>.
4. O usuário solicita informações privadas de seu perfil.
5. O servidor valida o JWT e decide se o usuário pode ou não acessar essa informações.

Nesse cenário temos um mecanismo de autenticação “stateless”. Nossos recursos protegidos terão apenas que verificar se um JWT válido foi fornecido no cabeçalho de autorização. Caso nosso token tenha todas as informações necessárias para aquela requisição, isso pode ajudar a reduzir drasticamente consultas no banco de dados. Lembrando que JWTs são credenciais de acesso e devem ser tratados com cautela, um maneira de proteger seu sistema é configurando a expiração do token para a menor data viável.

www.cotiinformatica.com.br