

Para saber mais: terminologias do JWT

Como você viu nessa aula, o JSON Web Token possui alguns elementos que podem não ser tão recorrentes. Alguns deles são:

Payload

O *payload* é uma das 3 seções do JSON Web Token. Esse é um termo muito utilizado no mercado, sem uma tradução literal muito boa.

Num contexto de transporte de mercadoria, *payload* significa a carga que efetivamente gera lucro. Por exemplo, um caminhão que transporta computadores carrega outras cargas, necessárias para a transmissão da mensagem, como motoristas e estepes, mas apenas os computadores serão efetivamente vendidos e gerarão lucro, ou seja, os computadores são o *payload*. Para um contexto de computação, o *payload* são os dados que realmente importam na mensagem, em comparação com cabeçalhos e assinaturas, que apenas existem para permitir a transmissão da mensagem.

Lá é possível guardar também informações como nome do usuário e a data de criação (*timestamp*) do token.

HMAC-SHA256

O **HMAC** (<https://pt.wikipedia.org/wiki/HMAC>) (*Hash-based Message Authentication Code*) é um tipo de **autenticador de mensagem** (MAC) (https://pt.wikipedia.org/wiki/Autenticador_de_mensagem) envolvendo uma função de *hashing* e uma chave secreta. Como a função de *hashing* usada, no caso, é a SHA256, o processo de geração desse código é chamado de HMAC-SHA256.

Ele é um dos algoritmos usados para a assinatura do JWT.

Base64URL

O **Base64URL** (<https://base64.guru/standards/base64url>) é uma variação da codificação **Base64** (<https://pt.wikipedia.org/wiki/Base64>), criado para permitir seu uso em nomes de arquivos ou endereços URL. Essa codificação é, então, usada no processo de criação do JWT.