Entendendo e Documentando RESTful APIs

Autenticação

Autenticação

“Autenticação é uma parte importante de qualquer aplicação Web moderna, ela tem a missão de identificar quem está usando a aplicação e se ela tem permissão para usá-la.”

Autenticação

“Alguns websites ainda gerenciam a autenticação através de cookies conforme a **RFC 6265** (`https://tools.ietf.org/html/rfc6265`)”

Autenticação

“Mas, cookies são criados para permitir o servidor gravar e manter os estados (**stateful**), o que é completamente contrário ao que o REST propõe (**stateless**), ou seja uma requisição não depende de outra.”

Autenticação

> “A ideia por trás do stateless é permitir aplicações web mais escaláveis e de fácil caching para serem mais efetivas.”

Autenticação

“O padrão do esquema de autenticação HTTP **basic** e através de **digest** são stateless, mas, atualmente muitas empresas precisam identificar seus usuários e querem diminuir a barreira para que eles usem seus produtos. Isso significa não ficar pedindo a senha do usuário frequentemente, de preferência apenas uma única vez.”

Autenticação

“Quando uma aplicação web oferece ferramentas para outras aplicações web através de API, a autenticação pode ser feita através de uma **API Key** ou **API secret token** como são conhecidas.”

Autenticação

“Em resumo, uma API Key é um combinação de letras e números bem grande, como um hash, e fica sendo transmitida em todas as requisições para identificar aplicação e geralmente é combinada com um email/senha.”

Autenticação

“Aqui vale uma ressalva. Como estas API Keys trafegam entre o servidor e o cliente, é importante que o servidor tenha configurado os **certificados SSL** (`https://letsencrypt.org/`) para garantir a maior segurança possível.”

Autenticação

“Diferentemente de aplicações, quando um usuário utiliza um serviço ele também deve ser identificado, geralmente com seu email/senha, mas, enviar esses dados a cada requisição com certeza não é o ideal.”

Autenticação

“Para tal, uma das soluções é no momento em que o usuário faz o login, o mesmo recebe um token baseados em suas credenciais e daí pra frente o token servirá de identificação nas próximas requisições.”