Glossário de Segurança

Sigla	Descrição	Informação
API	Interface de programação de aplicativo	Uma interface de programação de aplicativo é um conjunto de rotinas, protocolos e ferramentas para construir aplicativos de software. Uma API especifica como os componentes de software devem interagir
FAPI	Financial API	Especificação técnica de API e define requisitos técnicos adicionais para o setor financeiro
CIBA	Client Initiated Backchannel Authentication	A autenticação de backchannel iniciada pelo cliente (CIBA) é um dos padrões mais recentes da OpenID Foundation. São categorizados como "fluxo desacoplado". Permite novas maneiras de obter o consentimento do usuário final
OAuth		O OAuth é um protocolo de autorização para APIs web voltado a permitir que aplicações *client* acessem um recurso protegido em nome de um usuário
OIDC	OpenID Connect	OpenID Connect é um protocolo de identidade simples com padrão aberto

JWT	JSON Web Token	Uma técnica definida na RFC 7519 para autenticação remota entre duas partes. Ele é uma das formas mais utilizadas para autenticar usuários em APIs RESTful
JWS	JSON Web Signature	Uma forma de garantir a integridade das informações em um formato altamente serializado
SHA256	Secure Hash Algorithm	Um conjunto de funções criptográficas de hash
PKCE	Proof Key for Code Exchange	Chave de prova para troca de código por clientes públicos Oauth
MAC	Código de Autenticação de Mensagem	Permite que as declarações sejam assinadas digitalmente ou protegidas por integridade utilizando JWS
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira	Na definição oficial, “uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão"
AC	Autoridade Certificadora	
AR	Autoridade de Registro	
TLS	Transport Layer Security	
ECDSA	Elliptic Curve Digital Signature Algorithm	Algoritmo de método de assinatura digital de documentos utilizando criptografia baseada em curvas elípticas

ECDHE	Elliptic-curve Diffie–Hellman	Protocolo de contrato chave que permite que duas partes, cada uma com um par de chaves público-privado de curva elíptica, estabeleçam um segredo compartilhado em um canal inseguro
AES	Advanced Encryption Standard	Algoritmos de criptografia de bloco simétrico com uma chave de criptografia de 256 bits
Autenticação mútua		Chamamos de autenticação mútua quando ambos cliente e servidor apresentam certificados para serem validados pelo par
CSR	Certificate Signing Request	Contém informação que irá ser incluída no seu certificado como o nome da empresa/organização, common name (domínio), localidade e país. Também contém a chave pública (public key) que será incluída no seu certificado. Normalmente é também criada uma chave privada (private key) ao mesmo tempo que é criado o CSR
SSA	Software Statement Assertion	SSA é um JSON Web Token (JWT) que contém metadados sobre uma instância de aplicativo client desenvolvida por um TPP. O JWT é emitido

		e assinado pelo Diretório do Open Insurance Brasil
End User		Identificação de usuário final que possui as informações que se deseja acessar
Back-End		Aplicação ou código que da inteligência de negocio as ações solicitadas via API , código que efetivamente realiza a função desejada
Json	JavaScript Object Notation	Modelo para armazenamento e transmissão de informações no formato texto.
Claims		Escopos/declarações usadas em uma API durante a autenticação para autorizar o acesso aos detalhes de um usuário, como nome e imagem por exemplo. Cada escopo retorna um conjunto de atributos do usuário, que são chamados de declarações
Header		Cabeçalho de uma solicitação ou resposta que transmite contexto e metadados adicionais sobre a solicitação ou resposta. Por exemplo, em uma mensagem de solicitação podem ser usados para fornecer credenciais de autenticação
Payload		Carga Útil do token JWT. É aqui que você coloca informações como a quem o

		token pertence, qual a expiração dele, quando ele foi criado, entre outras coisas