

Cidadão.BR

Serviço de Identidade e Autenticação do Cidadão

Guia de Integração

Versão 1.0.0

Ridai Govinda Pombo / Fernando Vinícius de Magalhães

Protocolos que habilitam autenticação única

O Cidadão.BR foi projetado e implementado com foco em interoperabilidade, então respeita e segue os padrões de mercado para habilitar a autenticação única, ou *Single Sign-On*. O padrão mais proeminente e utilizado é *OAuth*, projetado para trabalhar com o protocolo HTTP e ele é essencialmente uma forma de permitir que *tokens* de acesso sejam emitidos para clientes terceiros por um servidor de autorização, com a aprovação do proprietário dos recursos (o usuário normalmente). O *OAuth* é complemento do protocolo *OpenID* e tem relação direta com o *OpenID Connect (OIDC)*, que é uma camada de autenticação construída em “cima” da versão 2.0 do *OAuth*.

Sob uma visão de fluxo, o *OAuth* é uma forma de delegação de acesso a API's. A versão 2.0 do *OAuth* provê fluxos de autorização para aplicações *web*, *desktop*, celulares e até dispositivos *IoT*. O *OAuth 2.0* não suporta, em sua especificação, assinatura digital, criptografia e verificação do cliente. Ele depende completamente do protocolo *TLS (Transport Layer Security)* para obter algum nível de confidencialidade e autenticação do servidor.

A especificação não dita nem detalha como se emitiria os *tokens*, qual seria seu formato, implementações específicas e etc. Para isso foi escolhido o padrão *JWT (JSON Web Token)*. Esses objetos são projetados para serem compactos, passíveis de serem enviados na URL e usáveis especialmente num contexto de SSO em navegadores. Ele é utilizado tipicamente para passar a identidade de usuários autenticados entre um provedor de identidade e um provedor serviço. Eles podem ser criptografados e autenticados.

Gateway de API

Os *tokens* emitidos pelo servidor de autorização, já autenticados pelo provedor de identidades do Cidadão.BR devem ser aceitos pelo usuário; ou seja, ele deve confirmar que autoriza a aplicação fim a ter acesso a informações necessárias pela aplicação. Por exemplo, a aplicação Meu INSS precisa acessar e ler o CPF, o NIT e o Nome completo; após autenticar com sucesso, o usuário precisará permitir o acesso a esses atributos, que compõe o *token JWT* emitido. Se ele não permitir, a aplicação não poderá trabalhar corretamente, então o usuário nem poderá acessar ela.

Os protocolos *OAuth 2.0* e *JWT* são utilizados no contexto de controle de acesso à API's, assim fica simples trabalhar com aplicações responsivas, híbridas e nativas de dispositivos móveis. Para simplificar a forma de trabalho, ter mais governança e interoperabilidade, cada infraestrutura dessas aplicações utiliza um *Gateway de API*, um tipo de software de *middleware* que controla o acesso às API dos serviços construídos e suportados. Aplicações internas à infraestrutura da Dataprev utilizam um *Gateway* na rede interna. Aplicações externas, terão que possuir seu próprio software, publicá-lo e suportá-lo na sua própria rede interna ou externa, conforme o caso.

Este *Gateway* receberá e manterá esses *tokens JWT*, aplicações que não mantêm estado precisarão armazenar o *token* recebido do servidor de autorização para que a cada invocação da API anexem o token, para continuarem autorizadas a utilizá-la.

Procedimento de integração

Para uma nova aplicação se integrar, é necessário que ela se identifique e que possua uma chave criptográfica que a autorize a atuar junto ao provedor de identidades e do servidor de autorização. Esse procedimento, no contexto do Cidadão.BR, é descrito abaixo:

1. Enviar um e-mail para a caixa cidadaobr.dtp@dataprev.gov.br, com as informações a seguir:
 - 1.1. Nome abreviado ou acrônimo que identifique unicamente a aplicação
 - 1.2. Descrição sucinta da aplicação ou serviços
 - 1.3. Descrição mais detalhada da aplicação
 - 1.4. Endereço (*URL*) da aplicação, na Internet
 - 1.5. Endereço (*URL*) de sucesso ou retorno após autenticação
 - 1.6. Definir as formas de liberação ou *grant type*, entre: implícito, por senha ou credenciais de cliente (*implicit, password, client_credentials*)
2. Aguardar o prazo máximo de 5 dias úteis para a configuração desta nova aplicação no *backend* do provedor de identidades e serviço de autorização do Cidadão.BR.
3. Será retornado a chave de criptografia específica para configuração da solução de "cliente" *OAuth 2.0*. A chave será enviada num arquivo .7z protegido por senha. A senha será a concatenação do nome abreviado da aplicação, os 6 primeiros caracteres da URL (após o <https://>), um hífen, os 6 últimos caracteres da URL de sucesso, outro hífen e uma sequência de 4 caracteres aleatórios que poderão ser recuperados entrando em contato telefônico com a equipe de Gestão de Serviço
 - 3.1. Essa chave é um segredo compartilhado para validação do *token JWT*, ele deverá ser gerenciado pelo *Gateway de API*

Contatos na Dataprev

Nome	Função	Telefone	E-mail
Alan do Nascimento Santos	Assessor de Diretoria	(61) 3207-3925	alan.santos@dataprev.gov.br
Beatriz Merguiso Garrido	Assessora	(61) 3207-3914	beatriz.garrido@dataprev.gov.br
Ridai Govinda Pombo	Gestor do Serviço	(21) 3616-8528	ridai.govinda@dataprev.gov.br
Maciel de Souza Moura	Substituto do Gestor de Serviço	(61) 3207-3403	maciel.moura@dataprev.gov.br
Marcelo Silva Santos	Gerente	(48) 3877-4745	marcelo.ssantos@dataprev.gov.br
"Equipe Cidadão.BR Dataprev"	Caixa Corporativa		cidadaobr.dtp@dataprev.gov.br