20º WRNP Workshop RNP | 6 E 7 DE MAIO GRAMADO | RS

GT-AMPTo - Autenticação Multi-fator para Todos

COORDENAÇÃO

Coordenador geral:
Prof. Emerson Ribeiro de Mello
Instituto Federal de Santa Catarina (IFSC)

Coordenador adjunto
Prof. Carlos Eduardo da Silva
Universidade Federal do Rio Grande do Norte (UFRN)

Coordenadora adjunta
Profa. Michelle Silva Wangham
Universidade do Vale do Itajaí (UNIVALI)

EQUIPE
Bruno Bristot (CIASC)
Felipe dos Passos Cardoso (IFSC)
Gabriela Cavalcante da Silva (UFRN)
Samuel Bristot Loli (IFSC)
Shirlei Aparecida de Chaves (IFSC)

PARCEIROS
GId-Lab - Laboratório de Gestão de Experimentação em Gestão de Identidade

SITE
gtampto.sj.ifsc.edu.br

CONTATO
mello@ifsc.edu.br

DESCRIÇÃO

O modelo de **gerenciamento de identidade federada** (*Federated Identity Management* - FIM) apresentou uma solução para o problema da proliferação de credenciais de acesso. Nesse modelo, cada usuário só precisa gerenciar uma única credencial de acesso e essa o permite acessar diferentes provedores de serviço. As soluções que implementam esse modelo também oferecem a facilidade de autenticação única (*Single Sign-On* - SSO). Nesse caso, o usuário só precisa passar pelo processo de autenticação uma única vez, junto ao seu provedor de identidade, independente de quantos provedores de serviço ele for acessar

Credenciais de acesso são geralmente classificadas nas seguintes categorias:

- **aquilo que você sabe** - como as senhas;
- **aquilo que você possui** - como um cartão inteligente;
- **aquilo que você é** - como a biometria do usuário.

Atualmente, credenciais de acesso baseadas no par {*nome de usuário, senha}* são as mais utilizadas nos mecanismos de autenticação. Sabe-se que essa solução possui diversas fragilidades, como por exemplo usuário escolher senhas fáceis, e suscetível a diversos ataques, como por exemplo *phishing*.

A **autenticação multi-fator**, as vezes chamada de autenticação com dois fatores (*two factor authentication* – 2FA), surge como uma solução para aumentar a robustez dos processos de autenticação e, geralmente, combina fatores das diferentes categorias apresentadas anteriormente. Nesse caso, parte-se do pressuposto que, mesmo que um atacante consiga comprometer um desses fatores, o grau de dificuldade aumenta muito com a necessidade de comprometer dois ou mais fatores.

O padrão **Multi-Factor Authentication (MFA) Profile** especifica quais requisitos um evento de autenticação com múltiplos fatores deve atender, bem como um contexto de autenticação SAML para expressar a autenticação multi-fator em SAML. O MFA Profile pode ser usado por Provedores de Serviço (SP) para requisitarem aos Provedores de Identidades (IdP) que autentiquem seus usuários com mais de um fator, ou mesmo pelos Provedores de Identidades para indicarem aos Provedores de Serviço que o usuário usou mais de um fator durante o processo de autenticação.

GT-AMPTo

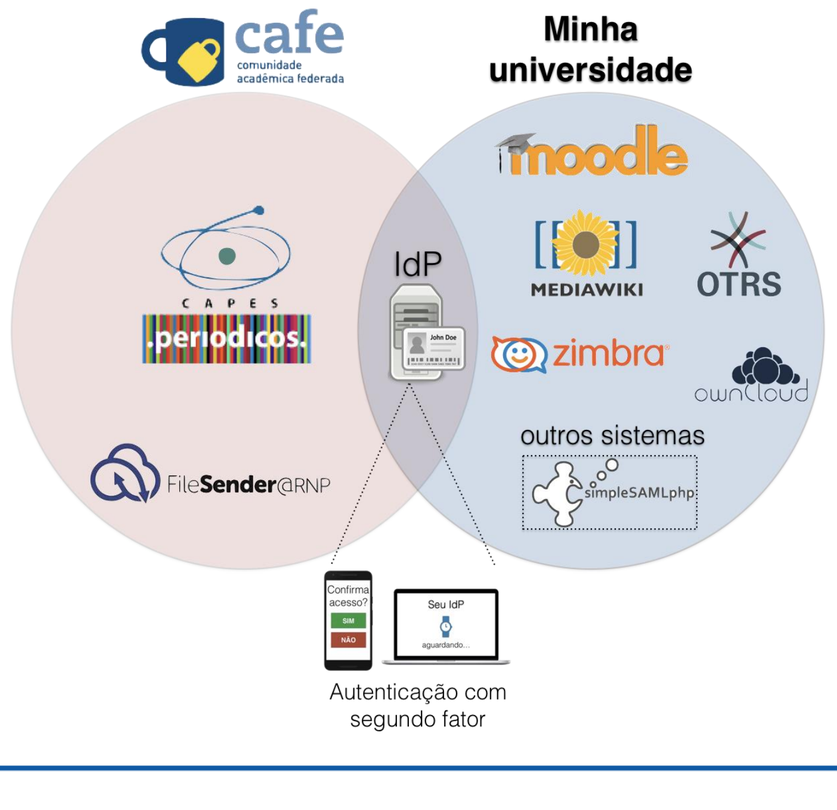
O objetivo do GT-AMPTo é permitir que Provedores de Identidade (IdP) da Comunidade Acadêmica Federada (CAFe), que fazem uso do SAML, autentiquem seus usuários com mais de um fator (i.e., senha, token, celular).

A solução tem como foco a usabilidade, facilidade para implantação e evolução e flexibilidade para que usuário possa escolher os fatores extras de autenticação que mais lhe agradar. A solução só precisa ser implantada nos provedores de identidade e não é necessário fazer qualquer tipo de alteração nos provedores de serviço.

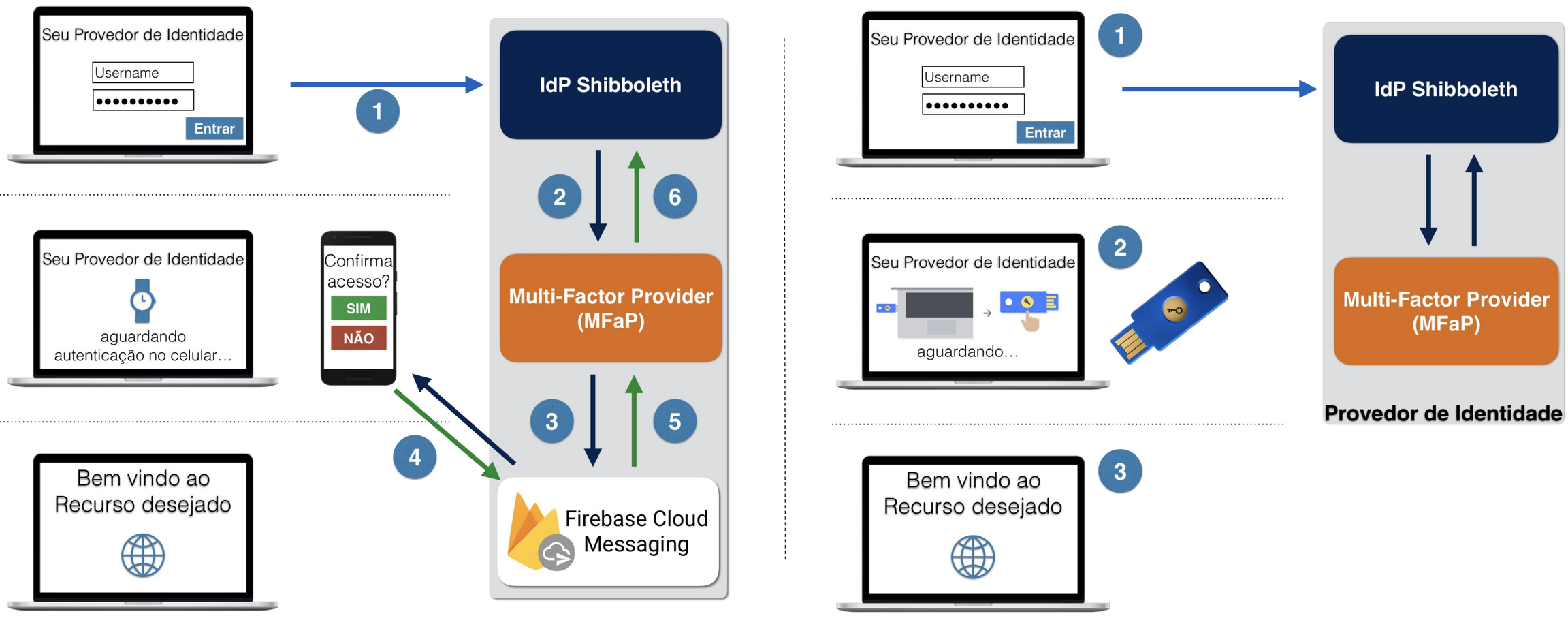
Atualmente a solução provê suporte para as seguintes tecnologias:

- **Diálogo de confirmação** - aplicativo para telefones inteligentes com foco na usabilidade;
- **Senhas descartáveis** (*One-Time Password* – OTP) - solução de 2FA amplamente usada por serviços comerciais e permite o uso de aplicativos como o FreeOTP, Google Authenticator e Authy;
- **FIDO2 USB Token** - padrão da indústria para autenticação robusta e presente nos principais navegadores web.

Instituições que fazem parte da CAFe podem usar a solução desenvolvida para ofertar autenticação com segundo fator em seus sistemas internos. Nesse caso, todos os sistemas int ernos deverão delegar a autenticação para o provedor de ide ntidade da instituição e deverão ser capazes de consumir ass erções de autenticação SAML.



Autenticação com segundo fator



Fluxo de autenticação usando o Diálogo de confirmação (esq.) e usando o FIDO2 USB token (dir.)

O **Diálogo de Confirmação** consiste de uma aplicação para telefone inteligente e durante os processos de registro e de autenticação é necessário que o usuário esteja com o celular próximo e que o mesmo possua conectividade com à Internet.

A autenticação com **Senhas Descartáveis (OTP)** depende de um telefone inteligente, porém o mesmo não precisa ter conectividade com à Internet.

O **FIDO2 USB Token** é uma solução de autenticação robusta e que não depende de um telefone inteligente ou mesmo de um dispositivo com conectividade com à Internet.

Para as três tecnologias, o usuário poderá usar o mesmo dispositivo (telefone + aplicativo ou usb token) com mais de uma conta de usuário em um mesmo provedor de identidade ou em provedores de identidade diferentes. Da mesma forma, o FIDO2 USB Token pode ser usado em provedores de serviço comerciais, como por exemplo, para autenticar em uma conta Google.

Como implantar a solução

A solução desenvolvida pode ser implantada na mesma máqui na onde está implantado o provedor de identidade da CAFe da instituição.

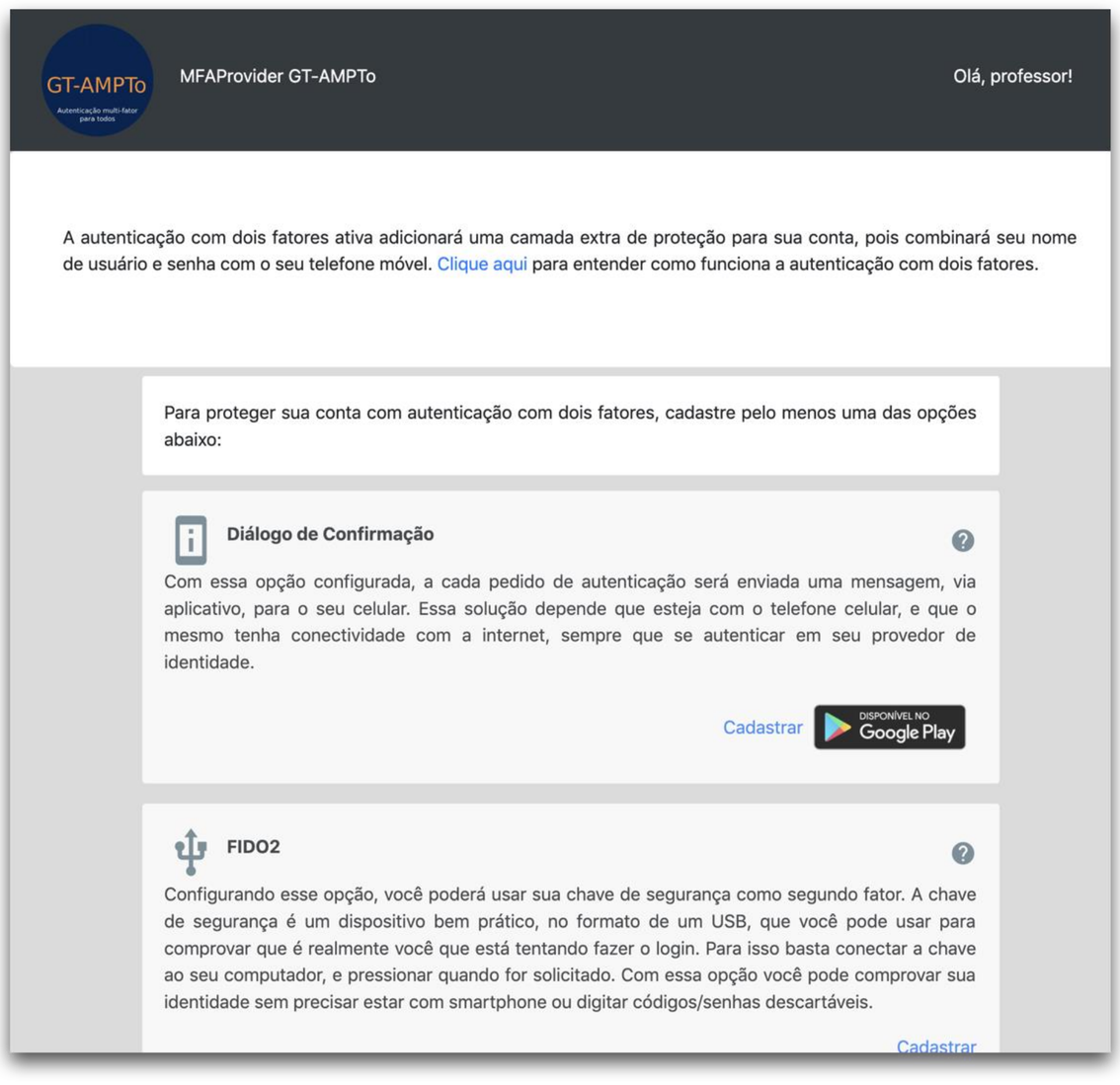
A instalação é feita por meio de *script* automatizado o qual tam bém pode ser usado para aplicar futuras atualizações. O admin istrador pode indicar quais tecnologias seus usuários poderão ativar como fatores extras de autenticação.

A instituição deverá possuir uma conta Google (gratuita) caso d eseje ofertar a solução de Diálogo de Confirmação para seus us uários. O aplicativo Diálogo de Confirmação será ofertado grat uitamente na Google Play Store e Apple Store pela Rede Nacio nal de Ensino e Pesquisa (RNP).

Uma vez implantado, cabe a cada usuário da instituição habilit ar a autenticação com dois fatores. Ou seja, a forma padrão de autenticação do provedor de identidade não é alterada e não é feita qualquer imposição para seus usuários.

O usuário tem acesso a um painel de controle onde poderá habilitar a autenticação com dois fatores e ainda indicar quais tecnologias serão seus fatores extras. O usuário poderá ter uma ou mais tecnologias habilitadas ao mesmo tempo.

Se o usuário perder acesso ao dispositivo que registrou como segundo fator, este precisará recorrer a códigos de *backup* (gerados durante o registro do segundo fator) ou, caso não os tenha por perto, precisará entrar em contato com o suporte de TI da instituição e esses serão capazes de desativar a autenticação com dois fatores.



Painel de controle para usuário gerenciar seus fatores extras de autenticação.

GT-AMPTo
Autenticação multi-fator para todos