Integração do *passkeys* em Provedores de Identidade Shibboleth

Andrey Adriano da Rosa[1*], **Emerson Ribeiro de Mello**[1]

[1]Instituto Federal de Santa Catarina - IFSC

andrey.a@aluno.ifsc.edu.br, mello@ifsc.edu.br

Abstract. *User authentication based on passwords is susceptible to various attacks and imposes a significant cognitive load on users. Multi-factor authentication seeks to minimize the effectiveness of certain remote attacks, but it often penalizes usability. Passkeys, a term coined based on recent standards from the FIDO Alliance and W3C, emerge as a robust alternative with a focus on usability for remote user authentication on the web. This work presents a solution for integrating passkeys into Shibboleth Identity Providers, enabling their use both as a second factor and as the first authentication factor.*

1. Introdução

A autenticação remota de usuários na *web*, baseada em senhas, está susceptível a ataques de *phishing* e força bruta. A autenticação com dois fatores, também chamada de autenticação multifator, busca combinar fatores de diferentes categorias (o que você sabe, o que você possui e o que você é) como forma de inviabilizar tais ataques. Segundo [Grassi et al. 2020, NIST 2017], a autenticação com dois fatores precisa empregar pelo menos um fator que seja resistente a ataque de *phishing*. A senha de uso único (*One Time Password*, OTP), por meio de aplicativos, envio por SMS, email ou chamada telefônica, é a tecnologia mais adotada pelos provedores de identidade na Internet. Contudo, OTP não é resistente a ataque de *phishing* e gera um passo extra para os usuários durante a autenticação, penalizando assim a usabilidade [de Mello et al. 2023].

Desde 2014 a *FIDO Alliance* vem atuando na proposição de padrões resistentes a *phishing*, baseados em criptografia de chave pública e sem dependência de Infraestrutura de Chave Pública (ICP), para aumentar a robustez do processo de autenticação remota de usuários na *web*. Contudo, não teve uma ampla aceitação, pois dependia de dispositivos dedicados (*i.e.* chaves USB) que não estavam amplamente disponíveis e não ofereciam uma solução adequada para a recuperação de acesso caso o usuário viesse a perder esse dispositivo. O FIDO *passkeys* [Alliance 2022] surgiu para resolver essa dificuldade, pois permite que as chaves criptográficas sejam sincronizadas por todos os dispositivos (*i.e.* telefones inteligentes, *laptops*) do usuário, de forma semelhante aos gerenciadores de senhas tradicionais.

A versão 4 do *Identity Provider Shibboleth*[1] (IdP) introduziu o conceito de módulos e *plugins* para permitir estender facilmente as funcionalidades do IdP. A

[*]Bolsista da RNP dentro do contexto do Comitê Técnico de Gestão de Identidade (CT-GId)

[1]https://shibboleth.atlassian.net/wiki/spaces/IDP4/overview

Rede Nacional de Ensino e Pesquisa (RNP) estendeu o IdP versão 4.2.1 para realizar a autenticação de usuários com dois fatores[2] com senha de uso único e códigos de emergência. A solução desenvolvida pela RNP[3] conta com um painel de segurança, onde cada usuário poderá configurar o segundo fator, e foi concebida de forma que seja fácil adicionar outras tecnologias para atuarem como um segundo fator de autenticação.

O presente trabalho tem por objetivo estender o código do IdP v4.2.1 da RNP para permitir usar o FIDO *passkeys* como uma tecnologia para segundo fator de autenticação e também, para permitir usar o FIDO *passkeys* como o único fator de autenticação do usuário, permitindo assim ser uma solução que não dependa mais das senhas.

2. FIDO *passkeys*

FIDO passkeys [Alliance 2022] surge como uma proposta para tornar mais simples e robusto o processo de autenticação remota de usuários na *web*, e em aplicativos móveis, removendo completamente a dependência das tradicionais senhas. Fundamentado sobre os padrões anteriores da *FIDO Alliance* e W3C, como a especificação WebAuthN [W3C 2021] e o protocolo CTAP [Lindemann et al. 2021], a solução é resistente a *phishing*, possui suporte nativo nos principais navegadores *web*, para *desktop* e dispositivos móveis, e busca resolver uma das principais inconveniências das tecnologias geralmente usadas como segundo fator, a perda do dispositivo que atua como segundo fator.

FIDO passkeys podem ser usadas como um único fator, substituindo a autenticação baseada em senhas e com a robustez de uma autenticação usando um fator resistente a *phishing*, ou também podem ser usadas como segundo fator, em situações em que seja desejado ou necessário manter o uso de senhas.

Para uso de uma *passkey* o usuário precisa realizar uma autenticação local em seu dispositivo, respeitando a forma que o usuário configurou seu dispositivo. Por exemplo, a autenticação local pode ser biométrica ou por meio do fornecimento do PIN do usuário.

As *passkeys* podem ser sincronizadas por todos os dispositivos do usuário, desde que esses façam parte de um mesmo ecossistema (*i.e.* Apple, Google ou Microsoft). Esse comportamento seria semelhante ao que acontece com os gerenciadores de senhas desses fabricantes. Assim como as senhas, as *passkeys* poderiam ser mantidas *online*, o que possibilitaria sua recuperação em caso de perda do dispositivo do usuário [GÉANT 2023].

A autenticação entre dispositivos, e mesmo entre ecossistemas, usando FIDO *passkeys* é viabilizada pela utilização do dispositivo móvel do usuário como um autenticador móvel. Neste cenário, o usuário pode autenticar-se em um dispositivo (*i.e laptop*) utilizando uma *passkey* salva em seu telefone inteligente. Nesse caso, o processo de autenticação inicia com o navegador no *desktop* apresentando um QRCode para que o usuário faça a digitalização com seu telefone móvel, onde está salva sua *passkey*, e é necessário que o *desktop* e o telefone móvel tenham uma interface de *Bluetooth* ativa (eles não precisam ser pareados). A interface *Bluetooth* é usada para garantir que o telefone, onde encontra-se a *passkey*, está próximo do computador de onde o usuário está tentando passar pelo processo de autenticação remota.

A sincronização de *passkeys* entre dispositivos é possibilitada pelo navegador ou

[2]https://ajuda.rnp.br/cafe/processo-de-adesao/adesao-idp/manual-de-instalacao-mfa

[3]https://busca.inpi.gov.br/pePI/servlet/ProgramaServletController?Action=detail&CodPedido=38555

sistema operacional daquele ecossistema (*i.e.* Apple, Google ou Microsoft), e possui funcionamento semelhante a de um gerenciador de senhas. No entanto, apesar de previsto, ainda não existem implementações que permitam sincronizar *passkeys* entre diferentes fornecedores, como Microsoft e Apple, sendo necessário ter ao menos uma credencial diferente em cada ecossistema [Alliance 2022].

3. Proposta

A proposta do trabalho é ofertar o *passkeys* como uma das tecnologias para autenticação de usuários em provedores de identidade Shibboleth. A implementação partirá do código do IdP MFA disponibilizado pela RNP, contudo será desenvolvido na forma de *plugin*, o que permitirá a solução ser implantada em IdP Shibboleth versão $\geq 4.2.1$ e < 5. Na Figura 1 é apresentado o fluxo de autenticação usando o *passkey* ou a senha de uso único como segundo fator de autenticação.

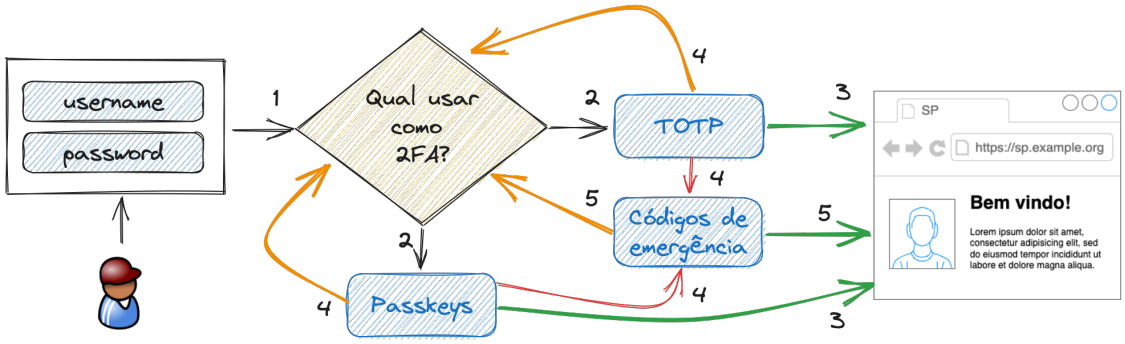

Figura 1. Fluxo de autenticação no IdP MFA com *passkey* ou TOTP como segundo fator

O usuário, ao configurar mais de uma tecnologia como segundo fator, indica qual delas será a tecnologia padrão durante o processo de autenticação. Assim, após passar pela autenticação por senha, o usuário deverá autenticar com TOTP ou *passkeys* (passo 2). Se a autenticação ocorrer com sucesso, ele obtém acesso ao recurso do provedor de serviço (passo 3). Caso não consiga se autenticar com a tecnologia padrão, então o usuário poderá escolher outra tecnologia (passo 4). Cabe citar que na implementação do IdP MFA da RNP a tecnologia "códigos de emergência" é para ser usada apenas caso o usuário não consiga se autenticar com o TOTP. Mas o usuário, uma vez estando na tela de autenticação com código de emergência, poderá ter sucesso e ir para o provedor de serviço (passo 5) ou poderá escolher outra tecnologia para se autenticar (passo 5).

O fluxo de autenticação com o *passkeys* como segundo fator será semelhante ao fluxo do TOTP, atualmente implementado no IdP MFA da RNP. Contudo, espera-se permitir o uso do *passkeys* como o único fator de autenticação, não dependendo mais de senhas. Dessa forma, será necessário criar um fluxo de autenticação especial dentro do IdP, além de criar uma página de configuração específica, dentro do atual painel de segurança do IdP MFA da RNP, para que o usuário possa habilitar o *passkeys* como único fator.

Pelo painel de segurança do IdP, o usuário poderá associar mais de uma *passkeys* a sua conta. Por exemplo, ele pode criar uma usando o ecossistema Apple e criar uma outra usando o ecossistema Google. Cada *passkeys* deverá ter um nome e o usuário fará uso desse para, por exemplo, saber qual *passkeys* irá excluir.

Todo o desenvolvimento dessa proposta será conduzido dentro da federação CAFe Expresso, disponibilizada pelo ambiente de experimentação GidLab[4] da RNP. O GidLab forneceu uma instalação completa e funcional do IdP MFA da RNP e o mesmo já encontra-se dentro da federação CAFe Expresso.

4. Conclusões

A FIDO *passkeys* é uma solução que eliminará a necessidade da autenticação baseada em senhas, entregando ao usuário uma experiência superior em termos de facilidades e usabilidade se comparada com os padrões FIDO anteriores e garantirá uma segurança robusta contra ataques de força bruta e *phishing*.

Este é um trabalho em desenvolvimento e espera-se que os resultados possam ser incorporados no IdP MFA da RNP, o que resultaria na disponibilização da facilidade de autenticação sem senha para todos os usuários das instituições que fazem parte da Comunidade Acadêmica Federada (Federação CAFe).

Referências

Alliance, F. (2022). How FIDO address a full range of use cases. https://fidoalliance.org/white-paper-multi-device-fido-credentials.

de Mello, E. R., Brito, A. E., Gomes, A. T. A., Schardong, F., Henriques, M. A. A., Wangham, M. S., de Chaves, S. A., and Silva, E. F. (2023). Relatório de visão de futuro em gestão de identidade. Publicações técnicas do Comitê Técnico de Gestão de Identidade (CT-GId) da RNP. https://wiki.rnp.br/download/attachments/106895177/CT-GId-visao-de-futuro-2023.pdf.

Grassi, P., Garcia, M., and Fenton, J. (2020). Nist special publication 800-63-3 digital identity guidelines. Technical report. https://doi.org/10.6028/NIST.SP.800-63-3.

GÉANT (2023). Introduction to passkeys usage and implementation. https://wiki.geant.org/display/GWP5/Passkey. Acesso em 4 de agosto 2023.

Lindemann, R., Brand, C., Czeskis, A., Jones, M. B., Hodges, J., Kumar, A., Powers, A., Verrept, J., and Ehrensvärd, J. (2021). Client to authenticator protocol ”(ctap)”. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html.

NIST (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b.

W3C (2021). Web Authentication: An API for accessing Public Key Credentials Level 2. https://www.w3.org/TR/webauthn.

[4]https://www.rnp.br/servicos/testbeds/gidlab