Autenticação multi-fator em provedores de identidade Shibboleth

Emerson Ribeiro de Mello[1], Michelle Silva Wangham[2], Samuel Bristot Loli[1], Carlos Eduardo da Silva[3], Gabriela Cavalcante da Silva[3]

[1]Instituto Federal de Santa Catarina (IFSC) – SC

[2]Universidade do Vale do Itajaí (UNIVALI) – São José – SC

[3]Universidade Federal do Rio Grande do Norte (UFRN) – Natal – RN

mello@ifsc.edu.br, wangham@univali.br, samuel.loli@ifsc.edu.br,

kaduardo@imd.ufrn.br, gabicavalcantesilva@gmail.com

Abstract. *Federated identity management model provides a solution for credencial access proliferation, such as based on passwords. However, it only takes the attacker to find out one password in order to personify the user in all federated service providers. The multifactor authentication emerge as a solution to increase the authentication process robustness. This work aims to present a comprehensive and open source solution in order to offer multifactor authentication to all Shibboleth Identity Provider users.*

Resumo. *O modelo de gerenciamento de identidade federada apresentou uma solução para o problema da proliferação de credenciais de acesso, por exemplo, baseada em senhas. Contudo, ao atacante basta descobrir a senha de um usuário para personificá-lo em todos os provedores de serviço da federação. A autenticação multi-fator surge como uma solução para aumentar a robustez dos processos de autenticação. Este trabalho apresenta uma solução completa e de código aberto para oferecer autenticação multi-fator para usuários de provedores de identidade Shibboleth.*

1. Introdução

Autenticação consiste em provar que um sujeito é quem afirma ser, normalmente, por meio de credenciais, tais como, nome de usuário e senha. A autenticação digital estabelece que um usuário que tenta acessar um serviço digital está no controle de uma ou mais credenciais válidas associadas à sua identidade digital [NIST 2017a].

Credenciais de acesso são classificadas nas seguintes categorias [NIST 2017a]: aquilo que você sabe – como as senhas; aquilo que você possui – como um cartão inteligente; aquilo que você é – como a biometria do usuário; e em [Brainard et al. 2006], é apresentada a categoria "alguém que você conhece" – relações humanas para intermediar a autenticação de um usuário. Para cada uma dessas categorias, tem-se vantagens e desvantagens que podem impedir o usuário correto de ter acesso ao recurso. Por exemplo, as senhas podem ser esquecidas, assim como um cartão inteligente pode ser perdido. A biometria não pode ser esquecida, mas pode ficar indisponível temporariamente, como a falta de voz, impressão digital apagada devido a um trabalho manual, etc. Além disso, apesar

da biometria apresentar maior disponibilidade, seu uso como único fator de autenticação não é considerado seguro, tendo em vista que as características de uma pessoa, apesar de serem únicas, são públicas, o que torna fácil a sua captura e construção de uma réplica.

O problema do roubo de identidade, isto é, o ato de se passar por um usuário usando credenciais roubadas, tem recebido crescente atenção por causa de seus altos custos financeiros e sociais [Bhargav-Spantzel et al. 2010]. Atualmente, credenciais baseadas no par "nome de usuário e senha" são as mais usadas pelos mecanismos de autenticação, apesar de suas fragilidades [Dasgupta et al. 2017]. Usuários podem escolher senhas fáceis, usar a mesma senha em múltiplas contas, escrever as senhas e etc. Além disso, atacantes tem a opção de usar diversas técnicas para roubar ou descobrir senhas, como por exemplo, *phishing*[1], ataques de força bruta, compra de senhas vazadas, entre outras técnicas [Aloul et al. 2009].

O modelo de gestão de identidade federadas permite a portabilidade da identidade digital através de diversos domínios [Arias-Cabarcos et al. 2015]. Neste modelo, o usuário precisa gerenciar apenas uma única credencial para acessar qualquer provedor de serviços (*Service Providers* – SP) da federação, uma vez que este usuário esteja autorizado pela política de controle de acesso do serviço em questão. O conjunto de especificações SAML (*Security Assertion Markup Language*) [Committee et al. 2012] se destaca na concepção de sistemas baseados neste modelo.

O modelo federado também oferece a conveniência da autenticação única (*Single Sign-On* – SSO), que permite ao usuário se autenticar em seu provedor de identidade (*Identity Provider* – IdP) uma única vez, independente de quantos provedores de serviços ele acessar. Neste contexto, o roubo de identidade é um problema sério, pois a autenticação única simplifica o trabalho do atacante, uma vez que um roubo de uma senha pode comprometer recursos de todos os SPs federados e, potencialmente, possibilitar o vazamento de dados sensíveis [Jensen 2012].

A autenticação multi-fator (*Multi-Factor Authentication* – MFA), às vezes chamada de autenticação com dois fatores (*Two Factor Authentication* – 2FA), surge como uma solução para aumentar a robustez do processo de autenticação. O MFA combina fatores de autenticação das diferentes categorias, apresentadas anteriormente, ou ainda dois ou mais fatores de uma mesma categoria, como é o caso das senhas descartáveis (*One-Time Password* – OTP) [Haller et al. 1998, M'Raihi et al. 2005]. 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 os demais fatores.

O objetivo deste artigo é descrever uma solução completa para que provedores de identidade Shibboleth possam realizar autenticação de seus usuários com múltiplos fatores de autenticação. O *framework* Shibboleth[2] segue o padrão SAML e é a solução mais adotada nas Federações Acadêmicas. A solução proposta foi construída sobre o padrão *Multi-Factor Authentication Profile* [Refeds 2017], garantindo assim a interoperabilidade com outras soluções de autenticação multi-fator que possam existir. A solução foi projetada para possuir baixo acoplamento com o IdP, para ser flexível para usuários e para

[1]Atacante pode induzir o usuário correto a fornecer suas credenciais de acesso em uma página *web* maliciosa.

[2]https://www.shibboleth.net/

administradores de IdP, e para ser extensível, permitindo que novas tecnologias sejam adicionadas como fatores extras de autenticação. O gerenciamento do ciclo de vida do segundo fator também é provido na solução proposta. Um protótipo da solução foi implementado e avaliado, considerando duas tecnologias como fatores extras de autenticação (Diálogo de confirmação e FIDO UAF [Machani et al. 2014]), além do desenvolvimento de um aplicativo para dispositivos Android.

O restante do artigo está organizado da seguinte forma. Na Seção 2 são apresentadas algumas tecnologias usadas para o desenvolvimento do trabalho. Os trabalhos relacionados são apresentados na Seção 3. Na Seção 4 é apresentada a solução proposta e o protótipo desenvolvido. Uma avaliação do protótipo desenvolvido é apresentada na Seção 5. Por fim, na Seção 6 são feitas as considerações finais, bem como os trabalhos futuros que serão explorados.

2. Contextualização Teórica

A autenticação com dois fatores (2FA) não é algo relativamente novo e está presente na maioria dos provedores de serviços comerciais. Atualmente, o método 2FA mais implementado se baseia no uso de senhas descartáveis (*One-Time Password* – OTP), obtidas por meio de aplicativos em dispositivos móveis (p.ex. *Google Authenticator* e Authy[3]), SMS ou ligações telefônicas. Contudo, o uso da rede de telefonia para envio de senhas descartáveis foi considerado como inseguro [NIST 2017a], uma vez que é possível personificar a estação do usuário, ou mesmo revelar a senha recebida por meio de um aplicativo malicioso em execução no telefone do usuário [Mulliner et al. 2013].

Em consequência da ascensão dos telefones inteligentes, tornou-se comum o uso de aplicativos para gerar senhas descartáveis [Aloul et al. 2009]. O uso de aplicativos reduz a dependência da rede telefônica e seus riscos, já que estes são baseados no algoritmo TOTP [M'Raihi et al. 2011] e independem da rede de dados para seu funcionamento.

A *Fast IDentity Online* (FIDO) *Alliance* foi criada com o objetivo de conceber padrões abertos para permitir construção de solução robusta para autenticação de usuários, baseada em criptografia de chave pública, de fácil uso e que não viola a privacidade dos usuários. A especificação FIDO UAF [Machani et al. 2014] permite a experiência sem senha, de forma que o usuário, usando a biometria, possa se autenticar localmente em seu dispositivo e transpor essa autenticação para os serviços remotos. A FIDO U2F [Srinivas et al. 2014] permite a experiência de autenticação com segundo fator de forma que o usuário não necessite de um dispositivo complexo, com interface rica e que precise de fonte de energia como um telefone inteligente.

Os provedores de serviço podem usar as especificações do FIDO UAF para desenvolver uma solução para atuar como o primeiro fator de autenticação, ou seja, o usuário não precisa, por exemplo, de uma senha como seu primeiro fator; ou ainda para atuar como segundo fator de autenticação. A solução proposta pela FIDO *Alliance* se baseia fortemente na confiança do provedor de serviço sobre o dispositivo que o usuário está usando durante o processo de autenticação. Neste caso, com o FIDO UAF assume-se que o usuário está de posse de um dispositivo como um *tablet*, telefone, relógio ou até mesmo um computador pessoal, certificado pela FIDO *Alliance*.

[3]https://authy.com/

Para um *hardware* ser certificado pela FIDO *Alliance*, esse deverá respeitar alguns requisitos de projeto, como por exemplo, fazer uso de ambiente de seguro de execução (*Trusted Execution Environment* – TEE) ou elemento seguro (*Secure Element* – SE) para armazenamento de material criptográfico. Por fim, todo *hardware* certificado terá seus dados publicados no serviço de metadados [Alliance 2016], mantido pela FIDO *Alliance*. Os provedores de serviços consultam esse serviço para determinar se confiam ou não na informação fornecida por um modelo de dispositivo.

A FIDO *Alliance* e o *World Wide Web Consortium* (W3C) uniram esforços para a construção de padrões para garantir uma autenticação forte em sítios *web* ou em aplicativos para dispositivos móveis, aproveitando assim muito da experiência com os padrões FIDO UAF e FIDO U2F. Dessa união surgiu o *Web Authentication* (WebAuthN) [W3C 2018] e FIDO2 *Client to Authentication Protocol* (CTAP) [Lindemann et al. 2017].

O WebAuthN define uma API para ser incorporada em navegadores e plataformas *web* e assim permitir que os serviços *online* usem a autenticação FIDO. Esta API permite a criação e o uso de credenciais baseadas em chave pública, por aplicativos *web*, com o objetivo de autenticar usuários de maneira segura. O FIDO2 CTAP permite que dispositivos externos, como telefones celulares ou *tokens* de segurança FIDO, usem o WebAuthN e sirvam como autenticadores para aplicativos de *desktop* e serviços da *web*.

Em 07 de junho de 2017, a REFEDS (the Research and Education FEDerations group) anunciou oficialmente o "REFEDS MFA Profile" [Refeds 2017]. O *MFA Profile* define os requisitos para um evento de autenticação com múltiplos fatores e como expressá-lo em um contexto de autenticação SAML. Um contexto SAML MFA pode ser usado por provedores de serviço para requisitar aos provedores de identidades que autentiquem seus usuários com mais de um fator e também pode ser usado pelos provedores de identidade para notificar os SPs que a autenticação com mais de um fator foi executada. O *MFA Profile* está presente no Shibboleth IdP desde a versão 3.3.1 e todas as soluções de autenticação multi-fator devem ser construídas, fazendo uso do mesmo.

3. Trabalhos Relacionados

Em [Weiser 1991], foi apresentada a visão de um mundo no qual a computação do século 21 seria móvel e onipresente. Pode-se concluir que isso se tornou realidade principalmente por causa dos telefones inteligentes (*smartphones*), que levaram a computação para o dia-a-dia dos usuários. Deste modo, os *smartphones* se tornaram um dos candidatos a dispositivo de suporte a autenticação multi-fator, como de fato já são usados por soluções comerciais, seja para recebimento de mensagens de texto (SMS) ou para executar algum aplicativo que permita o uso de senhas descartáveis [Aloul et al. 2009].

O *Google PhonePrompt* [Google 2017] surgiu como solução para os problemas de usabilidade e de segurança das soluções baseadas em senhas descartáveis. A solução, exclusiva para usuários dos serviços da Google, depende de telefones inteligentes e conectividade com à Internet. Atualmente, existem outras empresas que fornecem aos seus usuários uma solução semelhante ao *PhonePrompt*, como por exemplo: *Authy OneTouch* da empresa Authy, *Push-to-Accept* da empresa Secureauth[4] e o *DUO push*[5] da empresa DUO *Security*. Porém, todas são soluções proprietárias.

[4]https://docs.secureauth.com

[5]https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile

Dentre as soluções voltadas para o *framework* Shibboleth e que mais se aproximam da solução proposta neste artigo, destacam-se: FAME [Zhang et al. 2005]; *Multi-Context Broker* (MCB) [Langenberg 2015]; *Authentication Flow Selection* [Cantor 2015]; e o experimento prático descrito em [Morii et al. 2017]. Em [Zhang et al. 2005], foi proposto o *framework* FAME que possibilita a autenticação multi-nível e multi-fator no Shibboleth. No FAME é adicionada, na asserção SAML gerada, o nível de garantia (*Level o Assurance - LoA*) dos fatores de autenticação, utilizados para posterior aplicação do controle de acesso de granularidade fina. A integração da solução proposta com o *framework* Shibboleth exige a modificação do *Shibboleth Handle Service*, responsável por identificar e autenticar um usuário e, por ser uma solução mais antiga, não usa o *MFA Profile*.

Já os trabalhos MCB e *Authentication Flow Selection* estenderam os fluxos de autenticação do IdP Shibboleth de forma a permitir a autenticação com segundo fator. Contudo, no momento de suas concepções não havia uma especificação padronizada para indicar como realizar a autenticação 2FA e como expressar aos provedores de serviços que uma autenticação 2FA fora realizada. Sendo assim, as soluções desenvolvidas por estes trabalhos não garantem a interoperabilidade entre si ou com qualquer outra solução de autenticação com múltiplos fatores em IdPs Shibboleth. Importante ainda ressaltar que, ambas as propostas, dependem de soluções de terceiros, como da DUO *Security*[6], tanto para realizar a autenticação com segundo fator, quanto para fornecer o aplicativo que será usado como segundo fator pelos usuários.

Em [Morii et al. 2017], os autores descrevem um experimento prático que integra ao *framework* Shibboleth um sistema de autenticação externo sem senha baseado no FIDO2. Na solução, no processo de autenticação federada, o IdP Shibboleth redireciona o cliente do usuário (navegador *web*) para o servidor FIDO2. Nesse ponto o usuário se autentica localmente em seu dispositivo (p. ex. autenticação biométrica com Windows Hello) e o resultado dessa autenticação é transposta para o servidor FIDO2. Se a autenticação ocorrer com sucesso, então o servidor FIDO2 redireciona o cliente de volta para o IdP e esse último emite a asserção SAML com os atributos do usuário e a encaminha para o SP. A solução apresenta uma forma para permitir o uso do FIDO2 como o único fator de autenticação, porém, não oferece a possibilidade de autenticação com múltiplos fatores.

A presente proposta é uma solução completa, de código aberto e que não modifica o *framework* Shibboleth. Ou seja, apresenta componentes para estender os fluxos de autenticação do IdP Shibboleth para que suporte múltiplos fatores, além de fornecer um aplicativo que será usado pelos usuários como seu segundo fator de autenticação (da categoria aquilo que você possui). Por fim, a presente proposta segue uma especificação SAML padronizada para expressar informações sobre a autenticação com múltiplos fatores. A seção, a seguir, apresenta a proposta desenvolvida nesse trabalho.

4. Autenticação multi-fator em provedores de identidade Shibboleth

Antes da publicação do *MFA Profile* [Refeds 2017], não existia uma solução padronizada no Shibboleth para representar um evento de autenticação de usuário com mais de um fator. A solução proposta neste trabalho faz uso do *MFA Profile* e, até esta submissão, é a primeira solução de autenticação com múltiplos fatores de código aberto e completa,

[6]https://www.duosecurity.com

ou seja, sem dependência de serviços de terceiros, para provedores de identidade Shibboleth. Sabe-se o quão difícil é configurar, implantar e manter um provedor de identidade Shibboleth em um ambiente de produção. Dessa forma, foi concebida uma solução com baixo acoplamento do ponto de vista do provedor de identidade, o que possibilita uma fácil implantação e atualização tanto da solução quanto do *framework* Shibboleth.

Optou-se por desenvolver uma solução que garante flexibilidade, para usuários e para administradores de provedores de identidade, sobre quais tecnologias podem ser usadas como segundo fator de autenticação. Isto é, a solução foi projetada para permitir que um administrador do IdP indique quais tecnologias podem ser usadas como segundo fator por seus usuários. Ao usuário deste IdP, é dada a opção se este quer ou não ativar a autenticação com dois fatores e se sim, quais tecnologias, disponíveis em seu IdP, poderão ser seus fatores extras de autenticação. A solução foi projetada de forma que possa ser estendida, o que permite aos administradores de IdP implementar outras tecnologias para atuarem como fatores extra de autenticação.

Cabe citar que com a solução proposta não é necessário fazer qualquer tipo de modificação nos provedores de serviço (SP) para lidar com usuários que foram autenticados com dois fatores. Contudo, o *MFA profile* [Refeds 2017] também permite ao SP solicitar ao IdP para que autentique o usuário com mais de um fator de autenticação, e a solução aqui implementada também contempla essa funcionalidade.

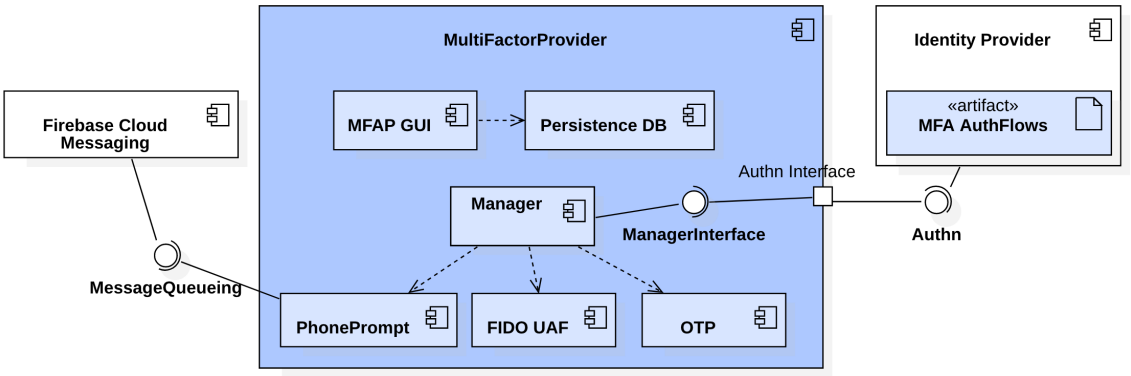

Figura 1. Diagrama de componentes UML da solução proposta

A Figura 1 apresenta um diagrama de componentes UML da solução proposta. O *Multi-Factor Provider* (MFaP), principal componente da solução, é uma aplicação Java que pode ser implantada no mesmo servidor de aplicação onde o Shibboleth IdP já está implantado. O Shibboleth IdP faz uso do *Spring Web Flow*[7] para orquestração de suas lógicas de negócio, o que inclui o processo de autenticação de usuários. Na configuração padrão do IdP, existe um fluxo padrão para autenticação e nesse fluxo são informadas todas as etapas necessárias para permitir autenticar um usuário, como: (1) como coletar credenciais; (2) validar, ou mesmo (3) solicitar novas credenciais. O IdP pode ser configurado com vários fluxos de autenticação e cada um deles possui uma identificação única. Os fluxos podem conter mais de um sub-fluxo ou interagir com outros fluxos de maneiras mais complexas, produzindo apenas um resultado final, que é modelado como um *AuthenticationResult* [Joie 2017].

[7]http://projects.spring.io/spring-webflow/

A versão 3.3 do Shibboleth IdP apresenta um fluxo próprio para configuração de autenticação multi-fator. Este fluxo fornece uma maneira programável de combinar diferentes fatores de autenticação para produzir uma sequência de desafios que se combinam. O fluxo MFA permite a adaptação e combinação de fluxos de autenticação, porém não define nenhum tipo específico de autenticação. Dessa forma, foram desenvolvidos fluxos de autenticação (*MFA AuthFlows*), essencialmente arquivos XML, e a partir deles o IdP consome os recursos REST, disponibilizados pelo MFaP, para realizar o registro dos fatores extras de autenticação e para realizar a autenticação, usando esses fatores.

Apesar do IdP ser responsável por realizar o processo de autenticação de seus usuários, as informações desses usuários (p. ex. login, senha, nome completo, etc.) são mantidas e obtidas de uma base de dados compartilhada por outros sistemas de informação da instituição. Tais informações, necessárias para autenticação de usuários, geralmente estão dispostas em um serviço de diretório (LDAP) ou mesmo em bases de dados relacionais.

Ciente de que cada instituição poderia ter uma base de dados em uma tecnologia diferente, foi proposta uma camada de abstração (componente `Persistence DB`) para persistências de dados relacionados aos fatores extras de autenticação dos usuários. Assim, as instituições poderiam manter as informações de autenticação em uma única base, não tendo que manter mais uma base de dados que seria específica para o MFaP. Na implementação, essa camada de persistência foi estendida para armazenar as informações dos usuários em uma base de dados não relacional (*NoSQL*).

Figura 2. Interface *web* do MFaP onde o usuário configura os fatores extras de autenticação.

O componente `MFaP GUI` consiste basicamente de uma interface *web* (ver Figura 2) onde o usuário poderá habilitar a autenticação com segundo fator, bem como configurar quais tecnologias poderão ser usadas como fatores extras de autenticação. Do ponto de vista do IdP, essa interface *web* do MFaP consiste de um provedor de serviço. Dessa forma, para que o usuário tenha acesso à interface *web* do MFaP, esse terá que passar pelo processo de autenticação junto ao IdP. O MFaP possui relação de confiança somente com o IdP onde está implantado, ou seja, somente usuários daquele IdP poderão

acessar sua interface *web*.

Por fim, o componente `Manager` provê a interface REST que é consumida pelos *MFA AutFlows* do IdP durante os processos de registro de segundo fator e de autenticação de usuários com o segundo fator. O componente `Manager` é responsável por instanciar objetos de acordo com a tecnologia usada como segundo fator. Como prova de conceito, o protótipo desenvolvido da solução proposta emprega as seguintes tecnologias como segundo fator: diálogo de confirmação e FIDO UAF [Machani et al. 2014], detalhadas nas próximas seções.

4.1. Diálogo de confirmação

As soluções de segundo fator baseadas no conceito de **Diálogo de Confirmação** objetivam aumentar a segurança do processo de autenticação de usuários, sem que isso cause um grande impacto na usabilidade. A ideia é semelhante as senhas descartáveis (OTP), porém sem a necessidade do usuário ter que digitar uma senha. O processo é simplificado de forma que o usuário só precise responder a um simples questionamento: "*Está tentando se autenticar em um outro computador? Sim ou não?*".

Soluções de Diálogo de Confirmação[8,9] [Google 2017] requerem obrigatoriamente um aplicativo no dispositivo do usuário e um serviço de fila de mensagens, responsável por intermediar as trocas de mensagens entre o provedor de identidade e o aplicativo no dispositivo do usuário. O *Firebase Cloud Messaging* (FCM)[10] oferece um serviço de troca de mensagens confiável e com baixo consumo de bateria para dispositivos Android, iOS ou mesmo aplicações *web*.

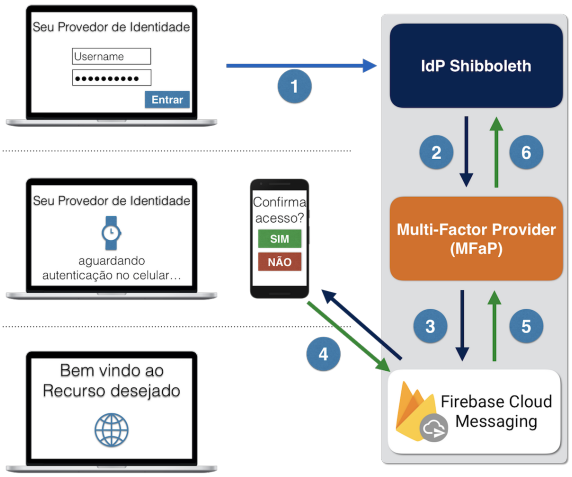

Figura 3. Troca de mensagens tendo o Diálogo de Confirmação como segundo fator de autenticação

Nesse trabalho foi desenvolvido um aplicativo para Android[11] e foi feito uso do FCM como solução para permitir a comunicação bidirecional entre o dispositivo do usuário e o IdP. Sendo assim, o usuário que desejar usar o Diálogo de Confirmação, como

[8]https://docs.secureauth.com
[9]https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile
[10]https://firebase.google.com/products/cloud-messaging/
[11]https://git.rnp.br/GT-AMPTo

seu segundo fator de autenticação, deverá: (1) instalar o aplicativo em seu telefone móvel; e (2) acessar a página *web* do MFaP para fazer o registro de seu aplicativo para atuar como o segundo fator. Nesse caso, o MFaP apresenta um QRCode que precisará ser lido pelo aplicativo presente no telefone móvel do usuário.

O QRCode fornecido pelo MFaP contém o EPPN[12], a URL do provedor de Identidade, além de um *nonce*. O aplicativo deve, então, enviar uma mensagem, via FCM, para o MFaP, fornecendo as informações que obteve do QRCode, além do identificador único de sua aplicação. Esse identificador será então usado para que o MFaP possa enviar notificações sempre que esse usuário passar pelo processo de autenticação, tendo o diálogo de confirmação como segundo fator.

Na Figura 3, é apresentada a troca de mensagens entre os componentes da solução durante a autenticação de um usuário que deseja acessar um provedor de serviço. No passo 1, o usuário fornece seu primeiro fator de autenticação em seu computador pessoal. O IdP verifica se este usuário possui 2FA habilitado e ao constatar que possui o Diálogo de Confirmação ativo, este encaminha o pedido ao MFaP para que o autentique com o 2FA (passo 2). O MFaP gera um *nonce* e o encaminha ao FCM (passo 3) para que esse último o entregue ao aplicativo instalado no celular do usuário. O usuário recebe uma notificação no celular, ou seja, ele não precisa, obrigatoriamente, estar com o aplicativo aberto, e clica no botão SIM (passo 4) para confirmar. A resposta do usuário é então encaminhada pelo FCM ao MFaP (passo 5) e chega ao IdP (passo 6), indicando que a autenticação 2FA ocorreu com sucesso. Por fim, o navegador do usuário é redirecionado para a página do provedor de serviço.

4.2. FIDO UAF

Apesar do Diálogo de Confirmação e FIDO UAF terem uma base tecnológica bem distinta, apresentam uma mesma experiência de uso ao pleitear acesso a um *site web*. No protótipo desenvolvido, pensou-se em um cenário onde não seria desejado ou mesmo possível fazer uso do par "nome de usuário e senha" e assim justificaria o uso do FIDO UAF como o único fator de autenticação. Dessa forma foi pensado no cenário de controle de acesso físico a salas em uma instituição. Na porta da sala existe um leitor de *smartcards*, o qual está conectado a um provedor de serviço Shibboleth que executa o perfil SAML ECP [TC 2008].

O aplicativo Android desenvolvido neste trabalho, além de ser usado para o cenário como diálogo de confirmação, também permite ao usuário cadastrar seu dispositivo como autenticador FIDO junto ao MFaP. Esse aplicativo ainda implementa a API *Host-Based Card Emulation* (HCE) para emular um cartão inteligente com suporte a tecnologia *Near Field Communications* (NFC).

Na Figura 4, são ilustradas as trocas de mensagens entre os componentes da solução durante a autenticação do usuário que está pleiteando o acesso a um ambiente na instituição. O processo de autenticação é iniciado assim que o usuário aproxima seu celular do leitor NFC e assim recebe o desafio FIDO (passo 1). O usuário se autentica localmente em seu dispositivo, fornecendo, por exemplo, sua impressão digital. O resultado da autenticação FIDO é então transposta para o MFaP/IdP, para realizar a autenticação

[12]eduPersonPrincipalName – identificador único do usuário dentro da federação

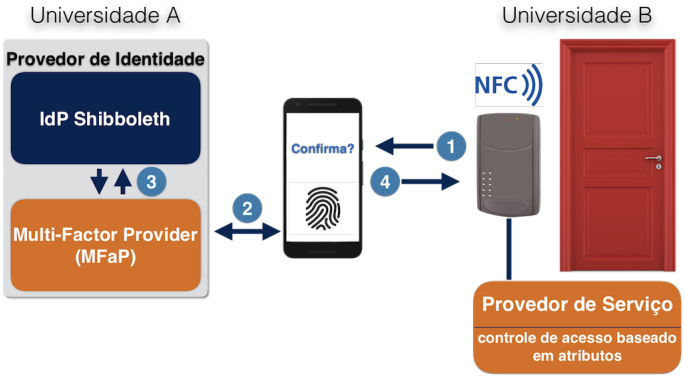

Figura 4. Autenticação de usuário usando o FIDO UAF como único fator de autenticação no cenário de controle de acesso físico.

junto ao IdP e obter a asserção SAML de autenticação (passos 2 e 3). Por fim, a asserção obtida é encaminhada ao SP (passo 4), o qual realizará a autorização, consumindo os atributos do usuário contidos na asserção SAML.

4.3. Gestão do ciclo de vida do segundo fator de autenticação

Durante o ciclo de vida de um fator de autenticação, é possível que aconteçam os seguintes eventos: associação, perda, substituição ou revogação. O procedimento adotado pela instituição para tratar cada um desses eventos poderá aumentar ou diminuir a robustez do processo de autenticação de seus usuários. Nesse trabalho parte-se do pressuposto que o usuário já possui um fator da categoria "aquilo que você sabe", associado a sua conta, aqui chamado de primeiro fator. Também assume-se que essas mesmas credenciais são usadas para que o usuário tenha acesso ao seu email, cenário típico das federações acadêmicas.

O processo de recuperação de acesso a uma conta que tenha segundo fator habilitado, e que o usuário tenha perdido esse segundo fator, difere para cada provedor de serviço. Contudo, observou-se que os *códigos de backup*, números que devem ser impressos pelo usuário, é a solução adotada por todos como a última alternativa, sem que precise envolver interação humana, para que o usuário consiga ter acesso a sua conta.

Na solução proposta, a associação do segundo fator de autenticação é feita por meio de um autosserviço, acessado pelo próprio usuário. Ou seja, para acessar esse autosserviço, pela primeira vez, o usuário precisará se autenticar somente com seu primeiro fator. A exploração desse autosserviço por um usuário malicioso poderia no máximo deixar um usuário correto impossibilitado de acessar sua conta. Nesse caso, a vítima poderia entrar em contato com a equipe de tecnologia da informação de sua instituição a fim de reestabelecer o acesso à conta.

A substituição do segundo fator pode-se justificar pela aquisição de um novo dispositivo físico ou mesmo pelo interesse em registrar uma outra forma de biometria (p. ex. substituir a impressão digital pelo reconhecimento facial). Na solução proposta, a substituição do segundo fator, ou seja, o registro de um novo e a revogação do atual, é feita pelo mesmo autosserviço apresentado acima. Nesse caso, para acessar o autosserviço, o usuário precisará se autenticar, obrigatoriamente, com os dois fatores que estão ativos no momento. Esse mesmo procedimento pode ser usado pelo usuário para adicionar outras tecnologias como fatores extras de autenticação.

A perda de um fator de autenticação impossibilita que o usuário consiga ter acesso a sua conta. Se a conta só estiver associado a um único fator, sendo esse uma senha, pode-se fazer uso de um autosserviço para recuperação da senha. Esse serviço pode enviar uma nova senha para o email do usuário; ajudar o usuário a lembrar da senha, por exemplo, mantendo o histórico das últimas senhas usadas; ou requisitar alguma informação do usuário, como perguntas de segurança ou dados pessoais. Contudo, se a conta do usuário estiver associada a um segundo fator de autenticação, da categoria "aquilo que você possui", o uso desse tipo de autosserviço pode ser desencorajado.

Segundo [NIST 2017b], ao se registrar um segundo fator de autenticação, recomenda-se registrar mais de uma opção para atuar como o segundo fator de autenticação, sendo que uma dessas opções seria usada como solução de *backup*. Na solução proposta, o usuário poderá definir uma ou mais tecnologias como fatores extras de autenticação e precisa indicar uma delas para ser sua tecnologia padrão para a autenticação com dois fatores. Se durante o processo de autenticação, o usuário ficar impossibilitado de usar o segundo fator padrão, este poderá escolher um dos demais fatores extras que habilitou. Cabe citar assim, que ao habilitar a autenticação com segundo fator, o MFaP gera automaticamente *códigos de backup*, senhas descartáveis para serem impressas, que o usuário poderá usar, caso perca o segundo fator padrão de sua conta.

A revogação de um fator de autenticação consiste em remover a associação deste na conta do usuário, impedindo assim que seja usado nos pedidos de autenticação subsequentes do usuário. Na solução proposta, somente o próprio usuário pode revogar fatores extras de autenticação que associou a sua conta ou ainda, desabilitar por completo a autenticação com dois fatores. Contudo, sabe-se que seria interessante o MFaP fornecer uma interface para que o administrador do provedor de identidade possa revogar os fatores extras de autenticação de seus usuários. Tal interface seria útil em casos onde usuários perderam acesso a sua própria conta ou mesmo para desativar por completo a conta de um usuário que não pertence mais à instituição.

5. Avaliação

Para a execução dos testes do protótipo, foram utilizados provedores de identidade e provedores de serviços disponibilizados pelo Laboratório de Gestão de Identidade (GIdLab)[13] da RNP. De maneira a avaliar a solução desenvolvida, foram elaborados planos de teste para as duas formas de autenticação implementadas (diálogo de confirmação e FIDO UAF) e para as operações de registro e de autenticação com o segundo fator.

O aplicativo Android desenvolvido permite atuar como fator extra de autenticação para mais de uma conta de usuário, podendo essas contas de usuários estarem em um mesmo provedor de identidade ou em provedores de identidade distintos. Os testes foram inicialmente executados com um único telefone Android e com uma única instalação do aplicativo desenvolvido, a fim de validar se o aplicativo se portaria corretamente diante do cenário de múltiplas contas de usuário, oriundas de um mesmo ou de diferentes provedores de identidade. Em outro conjunto de testes, foi feito uso de três telefones Android, de forma simultânea, a fim de verificar o comportamento da solução diante da concorrência de pedidos de registro de segundo fator e de autenticação usando o segundo fator.

[13]https://gidlab.rnp.br

A condução do teste de registro do diálogo de confirmação como segundo fator fora feita de acordo com os seguintes passos: (1) o usuário acessa página *web* do MFaP, após passar pela autenticação, usando o primeiro fator (usuário/senha) junto ao seu IdP; (2) o usuário clica na opção para habilitar o diálogo de confirmação; (3) o MFaP apresenta um QRCode que deve ser lido pelo aplicativo no telefone do usuário; (4) o usuário abre o aplicativo e lê o QRCode antes do código expirar e o aplicativo envia mensagem, via FCM, ao MFaP; (5) o MFaP e o aplicativo do usuário apresentam mensagem de sucesso.

O caso de teste descrito acima aconteceu com sucesso, bem como as seguintes variantes: (1) dois usuários de um mesmo IdP e um usuário de um outro IdP, usando três telefones distintos, tentam executar o registro do diálogo de confirmação; (2) um usuário clica na opção para habilitar o diálogo de confirmação, porém só lê o QRCode após o mesmo ter expirado. Nesse caso, o usuário não conseguiu registrar o segundo fator, sendo esse o comportamento esperado.

A condução do teste de registro do FIDO UAF se assemelha ao caso do diálogo de confirmação, exceto o fato de não necessitar da interação com o FCM. Foram executados testes com um único usuário, com três usuários e também o caso de ler o QRCode, após o mesmo ter expirado. Todos os testes apresentaram o resultado esperado.

Para a autenticação usando o segundo fator, foram conduzidos os seguintes casos de teste: (1) acessar um SP que não exige segundo fator, fazer uso de uma conta de usuário que tenha o segundo fator habilitado e se autenticar corretamente usando os dois fatores; (2) acessar um SP que não exige segundo fator, fazer uso de uma conta de usuário que tenha o segundo fator habilitado e não se autenticar corretamente com o segundo fator; (3) acessar um SP que exige o segundo fator e fazer uso de uma conta de usuário que não tenha o segundo fator habilitado. Todos os testes foram executados com sucesso, tanto para o diálogo de confirmação, quanto para o FIDO UAF.

6. Considerações finais

Este artigo apresentou uma solução para autenticação com múltiplos fatores em provedores de identidade Shibboleth. Até o presente momento, a proposta aqui apresentada consiste na primeira solução completa (que não depende de serviços de terceiros) de código aberto. Ou seja, a solução apresenta componentes para estender o fluxo de autenticação do IdP Shibboleth e apresenta um aplicativo para dispositivos Android atuarem como o segundo fator dos usuários. A solução desenvolvida segue fielmente o *MFA Profile* e pode ser facilmente incorporada a IdPs com o mínimo de impacto as instalações pré-existentes. Adicionalmente, a solução proposta permite a cada usuário indicar se quer habilitar ou não a autenticação com dois fatores e quais seriam as tecnologias dos fatores extras.

Os métodos diálogo de confirmação e FIDO UAF apresentam uma relação melhor entre usabilidade e segurança se comparado com métodos baseados em senhas descartáveis enviadas por meio de SMS. Contudo, os métodos escolhidos requerem que o usuário tenha um telefone inteligente e que este possua conectividade com a Internet, durante o processo de autenticação. Como trabalhos futuros, pretende-se implementar outros métodos para atuarem como fatores extras de autenticação, o que inclui: senhas descartáveis com TOTP [M'Raihi et al. 2011], FIDO U2F [Srinivas et al. 2014] e WebAuthN [W3C 2018]. A implementação desses métodos permitiria aos usuários terem fatores extras de autenticação independentes de telefones inteligentes ou de conectividade

com à Internet durante o processo de autenticação. Também pretendemos desenvolver um aplicativo para iOS para contemplar, a princípio, o cenário com o diálogo de confirmação.

Por fim, a solução não possui uma interface administrativa para gerenciar as contas que tenham habilitado o segundo fator de autenticação. Tal interface seria útil para lidar com aqueles usuários que perderam o dispositivo usado como segundo fator, bem como os códigos de *backup* e que estão impossibilitados de acessar suas contas para gerar novos códigos. Sendo assim, sugere-se essa interface como um outro trabalho futuro.

Agradecimentos

Agradecemos à Rede Nacional de Ensino e Pesquisa (RNP) pelo apoio e financiamento desse trabalho dentro do contexto do Grupo de Trabalho Autenticação Multi-fator para Todos (GT-AMPTo).

Referências

[Alliance 2016] Alliance, F. (2016). The FIDO UAF metadata service white paper. https://fidoalliance.org/wp-content/uploads/FIDO_Alliance_Metadata_Service_White_Paper_02122016.pdf.

[Aloul et al. 2009] Aloul, F., Zahidi, S., and El-Hajj, W. (2009). Multi factor authentication using mobile phones. *International Journal of Mathematics and Computer Science*, 4(2):65–80.

[Arias-Cabarcos et al. 2015] Arias-Cabarcos, P., Almenárez, F., Trapero, R., Díaz-Sánchez, D., and Marín, A. (2015). Blended identity: Pervasive idm for continuous authentication. *IEEE Security Privacy*, 13(3):32–39.

[Bhargav-Spantzel et al. 2010] Bhargav-Spantzel, A., Squicciarini, A. C., Xue, R., and Bertino, E. (2010). Multifactor identity verification using aggregated proof of knowledge. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(4):372–383.

[Brainard et al. 2006] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006). Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 168–178. ACM.

[Cantor 2015] Cantor (2015). Authentication flow selection. https://wiki.shibboleth.net/confluence/display/IDP30/AuthenticationFlowSelection#AuthenticationFlowSelection-FlowSelection.

[Committee et al. 2012] Committee, O. S. S. T. et al. (2012). Security assertion markup language (saml) 2.0.

[Dasgupta et al. 2017] Dasgupta, D., Roy, A., and Nag, A. (2017). *Multi-Factor Authentication*, pages 185–233. Springer International Publishing, Cham.

[Google 2017] Google (2017). Making google prompt the primary choice for 2-step verification. Google Official Blog. https://gsuiteupdates.googleblog.com/2017/10/making-google-prompt-primary-choice-for-2sv.html.

[Haller et al. 1998] Haller, N., Metz, C., Nesser, P., and Straw, M. (1998). Rfc 2289: A one-time password system. Technical report, Technical report, IETF.

[Jensen 2012] Jensen, J. (2012). Federated identity management challenges. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, pages 230–235. IEEE.

[Joie 2017] Joie, C. L. (2017). Authentication. https://wiki.shibboleth.net/confluence/display/IDP30/Authentication.

[Langenberg 2015] Langenberg, D. (2015). Multi context broker. https://spaces.internet2.edu/display/InCAssurance/Multi-Context+Broker.

[Lindemann et al. 2017] Lindemann, R., Bharadwaj, V., Czeskis, A., Jones, M. B., Hodges, J., Kumar, A., Brand, C., Verrept, J., and Ehrensvärd, J. (2017). Fido alliance proposed standard.

[Machani et al. 2014] Machani, S., Philpott, R., Srinivas, S., Kemp, J., and Hodges, J. (2014). Fido uaf architectural overview. *FIDO Alliance, December*.

[Morii et al. 2017] Morii, M., Tanioka, H., Ohira, K., Sano, M., Seki, Y., Matsuura, K., and Ueta, T. (2017). Research on integrated authentication using passwordless authentication method. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 682–685.

[M'Raihi et al. 2005] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and Ranen, O. (2005). Hotp: An hmac-based one-time password algorithm. RFC 4226, RFC Editor.

[M'Raihi et al. 2011] M'Raihi, D., Machani, S., Pei, M., and Rydell, J. (2011). Totp: Time-based one-time password algorithm. RFC 6238, RFC Editor.

[Mulliner et al. 2013] Mulliner, C., Borgaonkar, R., Stewin, P., and Seifert, J.-P. (2013). Sms-based one-time passwords: attacks and defense. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 150–159. Springer.

[NIST 2017a] NIST (2017a). Digital Authentication Guideline. *NIST Special Publication 800-63-3*. https://doi.org/10.6028/NIST.SP.800-63-3.

[NIST 2017b] NIST (2017b). Digital Identity Guidelines: Authentication and Lifecycle Management. *NIST Special Publication 800-63B*.

[Refeds 2017] Refeds (2017). Refeds mfa profile. https://refeds.org/profile/mfa.

[Srinivas et al. 2014] Srinivas, S., Balfanz, D., and Tiffany, E. (2014). Fido universal 2nd factor (u2f) overview. *Version v1. 0-rd-20140209, FIDO Alliance, February*.

[TC 2008] TC, O. S. S. (2008). Security assertion markup language (saml) v2.0. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[W3C 2018] W3C (2018). Web Authentication: An API for accessing Public Key Credentials Level 1. Technical report, World Wide Web Consortium.

[Weiser 1991] Weiser, M. (1991). The computer for the 21st century. *Scientific american*, 265(3):94–104.

[Zhang et al. 2005] Zhang, N., Yao, L., Chin, J., Shi, Q., Nenadic, A., McNab, A., Rector, A., and Goble, C. (2005). Plugging a scalable authentication framework into shibboleth. In *14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05)*, pages 271–276.