Uma proposta de adoção de autenticação baseada em Identidades Autossoberanas na RNP

Marco Aurélio Amaral Henriques

Faculdade de Engenharia Elétrica e de Computação
Universidade Estadual de Campinas (Unicamp)
13083-852 – Campinas, SP, Brasil

maah@unicamp.br

Resumo. *A federação CAFe tem prestado um grande serviço à comunidade de ensino e pesquisa brasileira, ao facilitar a autenticação federada de muitos usuários nos diversos serviços oferecidos tanto pela RNP como por outras instituições. Entretanto, existe um crescente movimento no sentido de dar aos usuários cada vez mais controle e autonomia sobre seus próprios dados e sobre o uso que é feito dos mesmos. Nesse contexto surgiu o conceito das identidades autossoberanas (SSI), no qual os usuários são os responsáveis pela guarda de seus dados e credenciais, liberando-os para provedores de serviço de uma forma mais transparente e controlada. Este trabalho busca discutir ideias para avaliar se e como o conceito de SSI poderia ser implementado gradualmente pela RNP de forma a permitir que usuários e instituições experimentassem essa nova forma de gestão de identidades e autenticação em paralelo com os sistemas atuais e com interferência mínima nos mesmos.*

1. Introdução

A maneira como usuários de diferentes serviços de TI se autenticam tem mudado com o passar do tempo [Allen, 2016]. Inicialmente era preciso que um usuário obtivesse credenciais diferentes para acessar cada serviço desejado, algo bastante trabalhoso em termos de gestão por parte do usuário e dos provedores de serviço. Além disso, era uma forma que trazia inseguranças para todos os envolvidos, já que parte dos usuários acabava repetindo uma mesma senha em diferentes serviços, comprometendo vários deles ao mesmo tempo quando tal senha era comprometida. Esse problema era agravado pelo fato de que os usuários normalmente não criam senhas seguras, mas sim senhas fáceis de memorizar, as quais acabam sendo inseguras por estarem provavelmente atreladas a algum dado do próprio usuário.

O problema da gestão de inúmeras senhas tem sido atacado em várias frentes, destacando-se duas abordagens distintas, mas vistas como praticamente idênticas pelos usuários. Uma delas é a adesão ao protocolo OpenId Connect por empresas com um grande número de usuários (tais como Google, Meta, Apple etc.). Isso permitiu que os provedores de serviço adotassem uma autenticação feita por uma entidade externa e aceitassem as credenciais fornecidas por tal entidade para garantir o acesso aos seus serviços. Assim, os usuários não precisaram mais criar credenciais em cada provedor de serviço e passaram a usar suas contas já existentes nas entidades externas para ter acesso ao serviço desejado. Apesar de ser conveniente, essa forma de autenticação tem problemas no tocante à centralização de dados de usuários em algumas poucas empresas e à falta de controle do usuário sobre tais dados, os quais podem ser usados de forma indesejada. Além disso, como tais entidades agregam um grande volume de informações pessoais de usuários, elas acabam se tornando um atraente alvo para atacantes que buscam obter dados pessoais para fins ilegítimos. Há ainda um outro problema nessa abordagem que pode ser ainda mais relevante: a privacidade do usuário fica fragilizada na medida em que, todas as vezes que ele faz uso de um dado serviço, a entidade de autenticação externa toma ciência e registra tal fato, o que pode ser usado para revelar diversas informações sobre esse usuário.

Uma outra abordagem para o problema das senhas individualizadas por serviço é a criação de federações de provedores de identidades. Essa solução foi mais amplamente

adotada por instituições de ensino e pesquisa e várias federações nacionais e internacionais foram criadas, como a CAFe - Comunidades Acadêmicas Federadas (Brasil), eduGAIN (Europa), ReFEDS (mundial) e Elcira (Europa e América Latina). Nesses casos, cada usuário precisa apenas ter as credenciais de autenticação em sua instituição de origem, a qual passa a disponibilizar para os provedores de serviço a autenticação de seus usuários por meio de um Provedor de Identidades (IdP). Sendo assim, um usuário em uma instituição participante da federação passa a ter acesso a todos os serviços disponibilizados para tal federação mediante autenticação no IdP de sua própria instituição. Apesar de ser uma solução menos sujeita a problemas de vazamento de dados e de ataques à sua privacidade, tais problemas não foram totalmente resolvidos e os usuários continuam sem controle total sobre suas informações. A CAFe e outras federações citadas neste parágrafo se baseiam no protocolo de autenticação SAML (*Security Assertion Markup Language*), que provê asserções de segurança entre os pares que o utilizam. Em vários aspectos, pode-se dizer que o que se faz com SAML é basicamente o mesmo que se faz com OpenID Connect (OIDC) citado anteriormente: permitir que um provedor de serviços terceirize a autenticação de seus usuários. Entretanto, no caso de OIDC não se vê uma distribuição da base de usuários entre as empresas que provêm autenticação pelo mesmo, já que cada uma delas que ter sua própria base centralizada de usuários. No caso da CAFe e outras federações, há um objetivo de aproveitar a possibilidade que os usuários já têm de se autenticar em suas instituições de origem, não reunindo todos em um só provedor de identidade e construindo, assim, uma real federação de identidades.

A proposta de Identidade Autossoberana (SSI) tenta amenizar todos os problemas apontados ao trazer para cada usuário a posse e a gestão de seus dados. Com o uso de novos conceitos como Identificadores Descentralizados (*Decentralized ID* - DID) e Credenciais Verificáveis (*Verifiable Credentials* - VC), os usuários passam a guardar consigo um conjunto de credenciais e de informações pessoais, as quais só são liberadas para um determinado provedor de serviços quando e se o usuário permitir. É o equivalente a tornar cada usuário seu próprio IdP, o que minimiza a dependência de informações armazenadas em servidores externos. Segundo [Reed et al., 2021], DID é um identificador que viabiliza identidades digitais descentralizadas verificáveis, podendo identificar pessoas, organizações, entidades abstratas etc. É projetado para ser independente de registradores centralizados, IdPs e autoridades certificadoras. Um esquema de Identidade Autossoberana tem características como gestão centrada no usuário, interoperabilidade digital, controle do usuário sobre a divulgação de identificadores, facilidade de uso em diferentes contextos, autonomia do usuário e possibilidade de agregar aos identificadores alegações confirmadas por terceiros, aumentando a confiabilidade da identidade digital [Toth and Anderson-Priddy, 2019].

Junto com o maior controle do usuário sobre seus dados vem o peso do custo e da maior responsabilidade pela guarda e gestão desses dados localmente, algo que os usuários estão habituados a delegar a terceiros. Se não forem tomadas medidas adequadas de educação e prevenção, o usuário pode vir a perder acesso a serviços devido a problemas de armazenamento de credenciais, falta de backup, falta de atualização de plataformas de software, incompatibilidades etc. No caso de SSI, o usuário não tem mais a quem recorrer em caso de problemas, pois foi trazido para si todo o ônus de cuidar de suas próprias informações em troca de ter mais transparência e mais controle sobre como seus dados são distribuídos. Nesse contexto surge a questão de o quão preparados e dispostos os usuários estão para assumir essa responsabilidade por cuidar de seus dados.

2. Uma proposta de implementação de SSI na RNP

Uma possível forma de responder objetivamente a questão anterior para o caso brasileiro seria disponibilizar em paralelo à Federação CAFe uma segunda forma de

autenticação baseada no conceito de SSI. Assim, instituições que desejassem experimentar tal conceito poderiam emitir credenciais para seus usuários guardarem consigo e apresentá-las quando solicitadas por um provedor de serviços. O uso de SSI precisaria ser opcional para os usuários também, já que nem todos estariam dispostos a adotar esse tipo de autenticação.

Do ponto de vista da RNP, poderia ser lançado de forma experimental um serviço de autenticação SSI para seus diferentes serviços. Entretanto, essa forma pode ser muito custosa, já que exigiria alterações nos serviços que hoje funcionam com base na autenticação federada sobre SAML. Uma forma alternativa seria tentar fazer uma integração temporária entre a Federação CAFe e o novo serviço de autenticação SSI, de maneira a não exigir alterações nos provedores de serviço atuais. Em outras palavras, a ideia é que não fosse feita nenhuma alteração na estrutura da federação, exceto nos IdPs que estão nas instituições. Tais IdPs seriam alterados de forma a oferecerem as duas formas de autenticação: a tradicional baseada em login e senha na instituição e uma nova baseada em técnicas de SSI. Em ambos os casos, a interação dos SPs com o serviço de descoberta (WAYF) e com tais IdPs seria a mesma e os SPs receberiam (após uma autenticação bem sucedida) exatamente os mesmos dados (asserções SAML) que recebem atualmente. Sendo assim, caberia ao novo IdP fazer toda a ponte e as conversões de protocolo necessárias entre as tecnologias atuais baseadas em Shibboleth de e para aquelas de SSI baseadas em DIDs e VCs.

Detalhando um pouco mais, a ideia é que, ao ser apontado por um usuário via WAYF, um IdP apresente duas opções de autenticação: a tradicional baseada em usuário/senha e uma nova baseada em SSI. Caso o usuário opte pela primeira, não haverá nenhuma diferença em relação ao fluxo normal de autenticação na CAFe. Caso o usuário opte pela segunda, o serviço IdP deve acessar um servidor de autenticação SSI como se fosse o usuário, usando os recursos disponíveis para autenticação externa presentes no código do servidor IdP SAML a partir da versão 4. Para isso, é necessário passar o endereço e porta sendo usados pelo navegador do usuário de forma que o servidor SSI possa iniciar com esse navegador o processo de autenticação SSI. Por questões de espaço, não poderemos entrar aqui em detalhes sobre o processo de autenticação SSI, o qual pode ser feito com várias plataformas disponíveis atualmente, tais como Hyperledger Indy Aries, Ion (Microsoft) e Jolocom, entre outros [Ferdous et al., 2019]. Do ponto de vista da integração entre os sistemas que está sendo proposta, o que importa é que, após esse processo de autenticação SSI o servidor de autenticação devolva para o IdP que o contactou um entre dois resultados possíveis: (i) uma mensagem de que a autenticação falhou, que será apresentada para o navegador do usuário pelo IdP, dando início a um novo ciclo de autenticação ou (ii) uma mensagem contendo os mesmos atributos que o IdP Shibboleth recebe da base de dados de usuários no processo tradicional de autenticação por usuário e senha (nome, email, CPF, data de nascimento etc.). Tais atributos devem estar presentes dentro de uma credencial verificável (VC) fornecida pelo usuário ao servidor de autenticação SSI e este deve reformatá-las de uma maneira que possam ser repassadas ao, e consumidas pelo, IdP. Após receber os atributos do usuário, o serviço IdP deverá seguir seu processo de autenticação tradicional, ou seja, criar asserções SAML com os mesmos e devolvê-las ao SP, o qual não perceberá nenhuma alteração no fluxo de autenticação atual e proverá o serviço inicialmente solicitado pelo usuário.

3. Vantagens e desafios

Como desafios para a implementação da proposta descrita, podemos listar: (i) criação da ponte entre o IdP e o serviço de autenticação SSI, já que são sistemas distintos no tocante a linguagens de programação, arquitetura de software e recursos para interoperabilidade; (ii) divulgação da iniciativa para as instituições e convencimento das mesmas para participar do projeto de experimentação com SSI; (iii) gerenciamento pela RNP de duas versões de IdP

(tradicional e com autenticação extra SSI); (iv) fornecimento para a instituição de um sistema alternativo de autenticação SSI composto por emissor de credenciais, servidor de autenticação e aplicativo móvel de guarda de credenciais: todo o software para essa estrutura SSI pode ser obtido de um projeto aberto como Hyperlegder Aries-Indy, por exemplo; (v) criação na RNP de infraestrutura de suporte às transações (blockchain, que também pode ser obtido do projeto Hyperledger Aries-Indy); (vi) fornecimento de treinamento sobre instalação, configuração e uso do novo IdP e do sistema de autenticação SSI; (vii) treinamento para os usuários sobre como gerir adequadamente as credenciais que passarão a guardar consigo (aplicativo móvel); (viii) coleta de informações com impressões dos usuários e gestores nas instituições sobre o uso da alternativa de autenticação SSI a fim de subsidiar decisões futuras sobre a adoção ou não dessa tecnologia. Como pontos positivos temos: (i) não obrigatoriedade de adesão para instituições ao modelo alternativo de autenticação SSI; (ii) não obrigatoriedade de adesão dos usuários das instituições que adotarem autenticação alternativa SSI; (iii) não necessidade de qualquer alteração em provedores de serviço (SP) Shibboleth atuais, sejam eles da RNP ou de terceiros; (iv) possibilidade de adesão gradual das instituições e de seus usuários ao modelo de autenticação SSI, na medida que entenderem ser de seu interesse fazê-lo; (v) provimento de uma forma relativamente simples e transparente de testar e avaliar as novas tecnologias envolvidas com autenticação SSI para determinar seus reais custos, vantagens e desafios em situações reais de autenticação de um grande número de usuários.

4. Conclusões

Com o advento de novas tecnologias de identificadores digitais descentralizados (DID) e de blockchains, tornou-se mais fácil a criação de um um sistema de autenticação autossoberana de usuários, mais fortemente centrada nos mesmos e dando-lhes controle total e transparência sobre os dados compartilhados com provedores de serviços. Este trabalho traz uma proposta inicial de adoção de arquiteturas de autenticação paralelas na RNP: a tradicional autenticação federada CAFe funcionando ao lado de outra baseada em identidades autossoberanas (SSI), de forma a permitir uma adoção gradual dessa última para avaliação e testes em situações concretas. Assim, tanto a comunidade de ensino e pesquisa como a RNP poderão decidir, com base em dados experimentais de campo, pela adoção ou não dessa nova tecnologia de identidades autossoberanas.

Referências

[Allen, 2016] Allen, Christopher. "The Path to Self-Sovereign Identity". *Life With Alacrity*.[Online]http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. último acesso em agosto, 2023.

[Reed et al., 2021] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, Markus Sabadello, “Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations”, W3C Draft, https://www.w3.org/TR/2021/WD-did-core-20210309, Março 2021.

[Toth and Anderson-Priddy, 2019] K. C. Toth and A. Anderson-Priddy, "Self-Sovereign Digital Identity: A Paradigm Shift for Identity," in *IEEE Security & Privacy*, vol. 17, no. 3, pp. 17-27, May-June 2019, doi: 10.1109/MSEC.2018.2888782.

[Ferdous et al., 2019] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nivel Superior – Brasil (CAPES) – Código de Financiamento 001.