Estudo experimental sobre Gestão de Identidades Autossoberanas para avaliação de riscos e oportunidades de adoção pela RNP

Bryan Wolff, Marco Aurélio Amaral Henriques

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

bryan.wolff@hotmail.com,marco@dca.fee.unicamp.br

Resumo. *A Identidade Autossoberana (SSI) é um padrão emergente baseado em credenciais verificáveis e identificadores descentralizados que surgiu da necessidade dos usuários terem controle absoluto e exclusivo de seus dados, que no ecossistema atual estão centralizados e em posse de terceiros. Essa nova arquitetura contribui para melhorias de privacidade e diminuição dos riscos de vazamentos. O objetivo deste trabalho é estudar, por meio de várias análises e experimentações, uma das principais soluções SSI e avaliar os riscos e oportunidades que sua implementação pode trazer para a RNP.*

1. Introdução

Todos os dias, as pessoas carregam carteiras cheias de cartões, porém, apenas alguns selecionados, como identidades governamentais, são amplamente aceitos. Para isso, a sociedade estabeleceu normas globais para saber como os cidadãos se apresentam e verificam as credenciais que esses cartões físicos representam. Mas não há um equivalente real para credenciais digitais. Porém, tudo isso está prestes a mudar, pois está surgindo uma nova forma de identidade digital, com base em padrões emergentes, como credenciais verificáveis e identificadores descentralizados, o que pode permitir que essas credenciais digitais funcionem em qualquer lugar, sejam mais confiáveis e contribuam para a privacidade de seus usuários.

A identidade digital é a forma como as pessoas (e em alguns casos, as máquinas) se apresentam de forma autêntica e confiável em canais digitais. As estruturas de qualquer sistema de identificação utilizado pelos meios digitais atualmente dependem exclusivamente do fornecimento de dados que ficam geralmente em posse de terceiros, longe do controle do usuário. Como a sociedade está cada vez mais ligada aos serviços online, estão também sujeitas a violações de dados e à perda de privacidade devido a falhas na correta identificação de atores em processos de autenticação, o que leva ao estabelecimento de canais de confiança onde um ou mais participantes não são de fato quem alegam ser.

No contexto de gestão de identidades, começaram surgir as ideias de que uma identidade digital deveria ficar totalmente sob o controle de seu dono e, então, consolidou-se o termo Identidade Autossoberana (ou SSI - Self-Sovereign Identity). Este novo sistema busca reestruturar o ecossistema de identidades digitais atualmente centralizado em algumas grandes empresas e instituições, transformando-o em uma arquitetura mais descentralizada e mais democrática.

2. Identidade Autossoberana (SSI)

Uma Identidade Autossoberana é uma forma de identidade descentralizada (DID - Decentralized ID). De acordo com Reed et al. [Reed et al., 2021], DID é um identificador que viabiliza identidades digitais descentralizadas verificáveis, podendo identificar pessoas, organizações, coisas, entidades abstratas etc. São projetadas para serem desacopladas de registradores centralizados, provedores de identidades e autoridades certificadoras. Podem até existir terceiros que auxiliem no processo de localização das informações relacionadas às DIDs, mas o detentor de uma DID deve ser capaz de provar o controle sobre a mesma usando técnicas criptográficas ou algum outro método de verificação sem requerer permissão ou depender de terceiros.

As principais características que devem estar presentes em uma Identidade Autossoberana são gestão da identidade centrada no usuário; interoperabilidade da identidade digital entre múltiplos prestadores de serviços; controle pelo usuário sobre como e para quem a identidade é fornecida; facilidade de transpor a identidade de um site para outros, não ficando amarrada a um único local; autonomia do usuário. Além disso, é desejável que uma Identidade Autossoberana permita que o usuário agregue à mesma alegações sobre si, suas capacidades e os grupos aos quais pertence. Tais alegações podem ser confirmadas por terceiros, dando mais confiabilidade ao que atesta a identidade digital [Toth and Anderson-Priddy, 2019].

Várias iniciativas foram criadas com esse objetivo, destacando-se as baseadas em tecnologia blockchain, que possuem propriedades desejáveis em uma SSI. Ferdous et al. [Ferdous et al., 2019] analisaram quatro sistemas de gestão de identidades descentralizadas baseados em blockchains: uPort/Serto (www.serto.id), Blockcerts (www.blockcerts.org), Jolocom [Fei et al., 2018] e Sovrin [Reed et al., 2019], concluindo que Sovrin é a plataforma com mais propriedades de uma SSI ideal. Além disso, outras novas propostas têm surgido, merecendo destaque o DIF – Decentralized Identity Foundation (identity.foundation) – e o recém lançado serviço de identidade descentralizada ION (identity.foundation/ion) pela Microsoft.

3. Objetivos do Trabalho

Este projeto objetiva fazer um estudo experimental das possibilidades e alternativas disponíveis para implantação de um sistema de Identidade Autossoberana na RNP. Tal estudo consiste em entender os reais benefícios e custos de um sistema de identidade digital baseado em identidade autossoberana, por meio da instalação, operação e avaliação de pelo menos uma plataforma de identidade autossoberana, como Jolocom, Sovrin ou ION. Com o apoio do GIdLab - Serviço de Experimentação em Gestão de Identidades da RNP, serão comparadas, de forma teórica e prática, as características, vantagens e desvantagens da gestão de identidade autossoberana com a gestão de identidade federada atualmente promovida pela RNP por meio da Federação CAFe.

4. Discussão

Os serviços web disponibilizado pela RNP utilizam-se de um modelo federado de gerenciamento de identidades conhecido como Comunidade Acadêmica Federada (CAFe). Nesse modelo, os usuários se autenticam utilizando o provedor de identidade (IdP) da sua própria instituição. Dessa forma, com apenas uma identidade digital, é possível ter acesso a diversos serviços disponibilizados pela federação. Porém, os dados do usuário ainda ficam sob o controle dos provedores de identidades em questão. Já um

modelo baseado em uma solução SSI não torna necessário o uso de um IdP institucional, pois os usuários passariam a se autenticar através de um programa aplicativo, onde gerenciam suas credenciais verificáveis que podem ser validadas com o uso de uma blockchain. Nesta perspectiva, o usuário possui mais controle sobre seus dados, obtendo as vantagens do uso de uma SSI.

A RNP (por meio do CT-Blockchain e do projeto ChainID) já tem alguns estudos em andamento sobre identidades descentralizadas com ênfase na plataforma Sovrin [Reed et al., 2019]. Neste trabalho, abordamos outras alternativas de sistemas de gestão de Identidades Autossoberanas baseadas em DID de forma a conhecer novas possibilidades oferecidas por diferentes tecnologias. Neste contexto, iniciamos os estudos da solução Jolocom [Fei et al., 2018], que foi desenvolvida sobre a blockchain da criptomoeda Ethereum e se baseia em contratos inteligentes. Os usuários fazem uso de um aplicativo móvel para interagir com o sistema a fim de criar, gerenciar e compartilhar suas identidades. É um protocolo de código aberto projetado de acordo com os princípios de uma SSI, permitindo que usuários individuais (sejam pessoas, organizações, dispositivos IoT etc.) criem, provisionem e controlem com segurança as suas identidades de forma autônoma e privada, ou seja, sem depender do provedor de serviços. A arquitetura desta solução segue as especificações básicas propostas pela normativa W3C (World Wide Web Consortium) referentes a Identificadores Descentralizados (w3c.github.io/did-core) e Credenciais Verificáveis (w3c.github.io/vc-data-model).

5. Resultados Preliminares

Em estudos iniciais, o protocolo Jolocom foi utilizado para criar identidades autossoberanas ancoradas (por *default*) na rede de teste Rinkeby da blockchain Ethereum. Assim, foi possível associar informações a essas identidades em forma de credenciais verificáveis, permitindo realizar interações entre elas para compartilhar e receber informações verificáveis. Esses fluxos de comunicação consistem em dois casos: emissão e verificação de credencial.

Para um serviço emitir uma credencial, quando solicitado, é necessário que ele crie uma oferta de emissão de credencial e transmita para aquele que a solicitou (cliente). Essa oferta inclui informações referente aos tipos de credenciais que o serviço pode emitir e é codificada como um JSON Web Token (JWT: datatracker.ietf.org/doc/html/rfc7519) para facilitar a comunicação e o consumo dos dados. Todas as mensagens de interação do protocolo podem ser enviadas a outros agentes para processamento por meio de outros canais como, por exemplo, um código QR a ser interpretado por um dispositivo com câmera. Ao receber essa oferta de emissão credencial, o cliente deve decodificar o JWT, verificar sua autenticidade e, em seguida, criar e enviar uma resposta contendo os tipos de credenciais desejadas. Ao receber a mensagem, o serviço a verifica, gera as credenciais solicitadas e as transfere para o cliente, novamente em formato JWT.

No caso de verificação de credencial, muitos serviços exigem que seus usuários forneçam certas informações no momento da inscrição ou autenticação. Isso é feito criando e transmitindo o que é chamado de “solicitação de apresentação de credencial”. Essa solicitação contém informações referentes ao tipo de credencial exigida, sendo também codificada em um JWT. O cliente deve decodificar o token, verificar sua autenticidade e criar uma resposta, contendo as credenciais exigidas durante este processo de verificação, codificadas em outro JWT. Ao receber a resposta, o serviço

deve decodificar, verificar sua autenticidade e verificar se o cliente passou as credenciais necessárias para a verificação. Se as condições do serviço forem satisfeitas, o usuário é autenticado e tem acesso ao serviço solicitado.

Para uma compreensão mais profunda do protocolo, é necessário instalar, operar e avaliar as ferramentas do Jolocom, o que está sendo feito em máquinas locais e outras disponibilizadas pelo GIdLab-RNP, onde são testados os fluxos de interação descritos anteriormente. Em uma implementação preliminar, foi utilizado o framework Express (expressjs.com/pt-br) para Node.js (nodejs.org), de código aberto sob a Licença MIT, que fornece recursos para construção de servidores web simples. Dessa forma, está sendo implementada uma plataforma simples de testes para emissão e verificação de credenciais, sendo toda a comunicação feita por meio de mensagens HTTP.

6. Conclusões e Trabalhos Futuros

A identidade digital, como utilizada atualmente, possui várias desvantagens quando se trata de privacidade, segurança, autenticidade, consentimento, escalabilidade e autonomia, as quais podem ser superadas com o auxílio da tecnologia SSI. As características de um sistema ideal baseado em SSI estão presentes na solução Jolocom, que teve um bom desempenho em testes iniciais. Como próximos passos, avaliaremos uma implementação mais completa dessa ferramenta e compararemos com o esquema de autenticação federada CAFe. Espera-se que este trabalho ofereça subsídios para uma discussão mais aprofundada das perspectivas e oportunidades de futura adoção da tecnologia SSI pela RNP.

Agradecimentos ao Programa de Gestão de Identidades 2021 da RNP pelo apoio.

Referências

[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.

[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.

[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 Working Draft, https://www.w3.org/TR/2021/WD- did-core-20210309, Março 2021

[Fei et al., 2018] C. Fei, J. Lohkamp, E. Rusu, K. Szawan, K. Wagner and N. Wittenberg. (Mar. 9, 2018). *Jolocom Whitepaper*. https://jolocom.io/wp-content/uploads/2019/12 /Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf. Último acesso em abril, 2021.

[Reed et al., 2019] D. Reed, J. Law and D. Hardman. (Sep. 29, 2016). *The Technical Foundations of Sovrin*. [Online] https://www.evernym.com/wp-content/uploads /2017/07/The-Technical- Foundations-of-Sovrin.pdf. Último acesso em abril, 2021.