Um estudo da relação custo/benefício de autenticação via Identidades Digitais Autossoberanas

Palavras-Chave: Identificadores Descentralizados, blockchain, gestão de identidades

Giovanni Machado Quintella Gama, DCA – FEEC

Prof. Dr. Marco Aurélio Amaral Henriques (orientador), DCA – FEEC

INTRODUÇÃO

Em várias situações no mundo real, precisamos apresentar informações sobre nós mesmos ao interagirmos com terceiros. Para fazer isso, demonstramos alguma evidência pessoal, isto é, asseguramos alguma informação própria, como quando dizemos nosso nome em encontros sociais, ou quando exibimos documentos emitidos por alguém confiável (governos, empresas, etc.), provando que a informação ali presente é legítima. Em retorno, aqueles com quem interagimos avaliam as informações que apresentamos e, se forem aceitas, criam um identificador, que será utilizado quando executarmos novamente o serviço, como, por exemplo, o banco te entrega um cartão para acessar sua conta em futuras situações.

Na internet, o mecanismo mais comum para identificar quem você é consiste na combinação de usuário e senha, credenciais criadas a cada novo serviço utilizado. Porém, surgem problemas nesse contexto: muitas senhas são difíceis de gerenciar, senhas fracas deixam informações vulneráveis a ataques e usar a mesma senha em vários serviços aumenta o risco de comprometimento das contas.

Uma das metodologias mais utilizadas na atualidade para sanar estes problemas é baseada em provedores de identidades (IdPs - Identity Providers), como Facebook ou Google, para manusear as credenciais. Sítios menores utilizam de tais IdPs para a autenticação e obtenção de informações básicas de identidade como nome e e-mail de seus usuários. O problema com esta opção é que cada vez que algum IdP é utilizado ele coleta informações sobre seus usuários; em consequência disso nossa privacidade é comprometida e nossos dados são monetizados por outros. O mais recomendado seria adaptar de alguma forma o modelo mais utilizado no mundo real para o mundo digital: o modelo de credenciais verificáveis em papel.

Esse modelo de credenciais é amplamente utilizado há muito tempo pela humanidade; entretanto, devido à facilidade de falsificação com ferramentas como o *Photoshop*, ele não pode ser diretamente aplicado no mundo digital. Ainda assim, podemos estudar seus princípios e procurar aplicar algo semelhante nesse novo mundo virtual. Entrando mais a fundo neste cenário, vemos que uma credencial seria uma declaração de alguma informação emitida para uma entidade (indivíduo ou organização) por um terceiro que tem a competência de fazê-lo; exemplos seriam CNH (Carteira Nacional de Habilitação), passaporte e diplomas, entre outros.

Uma CNH é emitida por uma autoridade governamental (o emissor) depois de você comprovar ser de fato quem é (normalmente com outra credencial) e que tem capacidade para dirigir. Você então mantém sua credencial, normalmente em sua carteira, e apresenta para qualquer um que necessite saber que você pode dirigir. Também é possível utilizá-la em outro lugar quando for necessário, como, por exemplo, abrir uma conta em um banco. Sempre que a credencial é apresentada, você está provendo a credencial para um verificador, que confere o documento e decide se ele é válido ou não para a situação em questão. Note que, nesses casos, o emissor não é chamado para participar na interação e é de total controle do dono da credencial se vai ou não apresentar a mesma e compartilhar suas informações.

IDENTIDADES AUTOSSOBERANAS

Credenciais Verificáveis (CVs) são atributos digitais assinados criptograficamente por autoridades, que se podem utilizar para comprovar que algo ou alguém realmente é quem supomos ser. Os dados são equivalentes aos papéis na vida real. Entretanto, a presença das assinaturas criptográficas dos emissores torna as CVs muito úteis no meio *online*. Os verificadores não precisam olhar fisicamente para o próprio documento ou uma versão escaneada dele para determinar quem o emitiu, se ele foi emitido para a pessoa que o apresenta ou se foi modificado de forma fraudulenta. Como resultado, o problema do verificador ter que confiar no titular de certa forma desaparece. O titular não está mais autoafirmando os seus dados e não pode forjar a criptografia que protege as credenciais. Assim, as credenciais podem ser aceitas como legítimas desde que o verificador consiga comprovar a assinatura do emissor.

Assim surge o modelo de Identidades Autossoberanas (SSI - Self Sovereign Identity), onde a ideia é que os dados sejam entregues para, e controlados somente pelo seu legítimo dono. Isso inclui a decisão de quando e como tais dados serão compartilhados com terceiros e, se forem compartilhados, como isso deve ser feito de maneira a garantir a segurança. Com SSI não há a presença de uma autoridade central que mantém todas as informações e as passa para outros quando são requisitadas.

Identificadores Descentralizados (DID – *Decentralized ID*) são um tipo de identificador que viabiliza identidades digitais descentralizadas verificáveis, podendo identificar pessoas, organizações, entidades abstratas etc. [1]. Foi projetado para ser independente de registradores centralizados, IdPs e autoridades certificadoras. Ainda existem terceiros que auxiliam no processo de localização das informações relacionadas aos DIDs, mas o detentor de um DID deve ser capaz de provar o controle sobre ele usando técnicas criptográficas ou algum outro método de verificação sem requerer permissão ou depender de terceiros.

A ideia de Identidade Autossoberana se baseia em algumas características essenciais, incluindo gestão centrada no usuário, interoperabilidade digital, controle do usuário sobre a divulgação de identificadores, facilidade de uso em diferentes sítios e autonomia do usuário. Além disso, SSI permite que o usuário agregue alegações confirmadas por terceiros, aumentando a confiabilidade da identidade digital [2]. Um fluxo simplificado de emissão e uso de CVs é mostrado na Figura 1.

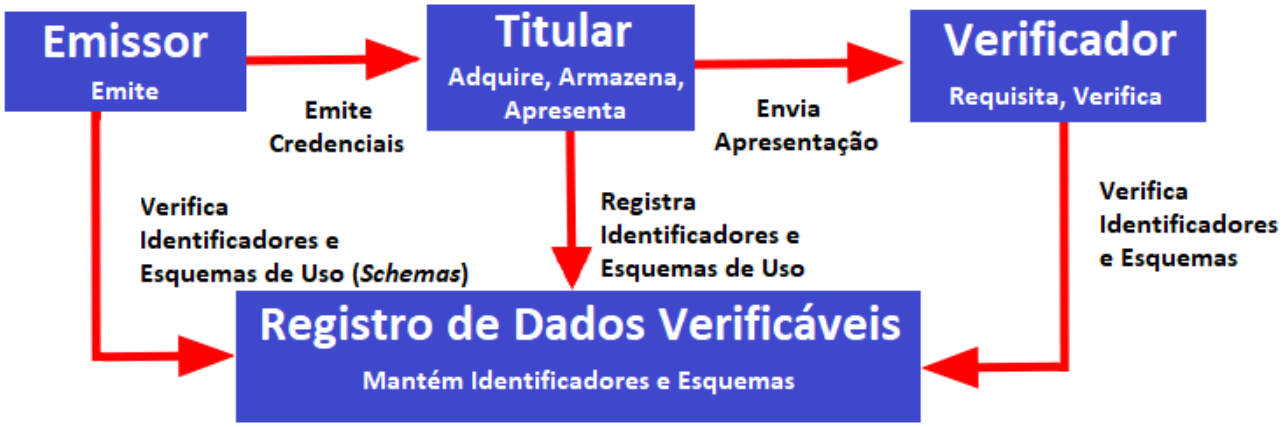

Figura 1. Representação do modelo de *SSI* e seus principais atores

Com o objetivo de criar sistemas de gestão de identidades descentralizadas (SSI), várias iniciativas têm sido desenvolvidas. As tecnologias de blockchain são amplamente utilizadas nessas soluções devido às suas características de descentralização, alta disponibilidade e garantia de imutabilidade. Entre os sistemas analisados por Ferdous et al. [3], destacam-se uPort/Serto, Blockcerts, Jolocom e Sovrin (implementado pelas tecnologias da Hyperledger). Este último é considerado a plataforma com maior aderência às propriedades desejáveis de uma SSI. Além dessas iniciativas,

outras propostas têm surgido no campo da identidade descentralizada, como a Decentralized Identity Foundation (DIF) e o serviço de identidade descentralizada ION, lançado recentemente pela Microsoft. Essas abordagens inovadoras estão avançando o campo da gestão de identidades descentralizadas e contribuindo para o desenvolvimento de soluções mais robustas e seguras.

Já é bem conhecido e adotado em várias situações o Projeto Hyperledger de código aberto para blockchains. Ele começou a ser aproveitado no mundo de gestão de identidades em 2017, com a criação da Hyperledger Indy, o primeiro ambiente inteiramente dedicado a identidades, tendo uma forte contribuição da Fundação Sovrin (https://sovrin.org). Com o passar dos anos, esse ambiente foi sendo separado em várias camadas para uma maior flexibilidade de uso em aplicações. Assim surgiram: Ursa, uma camada focada em criptografia; AnonCreds, um mecanismo de CVs baseado em ZKPs (Zero Knowledge Proof); Indy, implementação de uma blockchain pública e permissionada projetada especificamente para casos de uso de identidade descentralizada e, por fim, Aries, a parte dos agentes do grupo Hyperledger.

Em conjunto, Indy, Aries, AnonCreds e Ursa formam a *Hyperledger Identity Stack*, mostrada na Figura 2. Uma propriedade chave para a escolha desse protocolo é a flexibilidade dessa pilha: AnonCreds pode ser utilizada com outras soluções de camada 1 e 2; Aries pode ser utilizada com outras implementações de trocas de credencial de camadas 1 e 3; e a Indy pode fornecer suporte para outras implementações em camadas superiores.

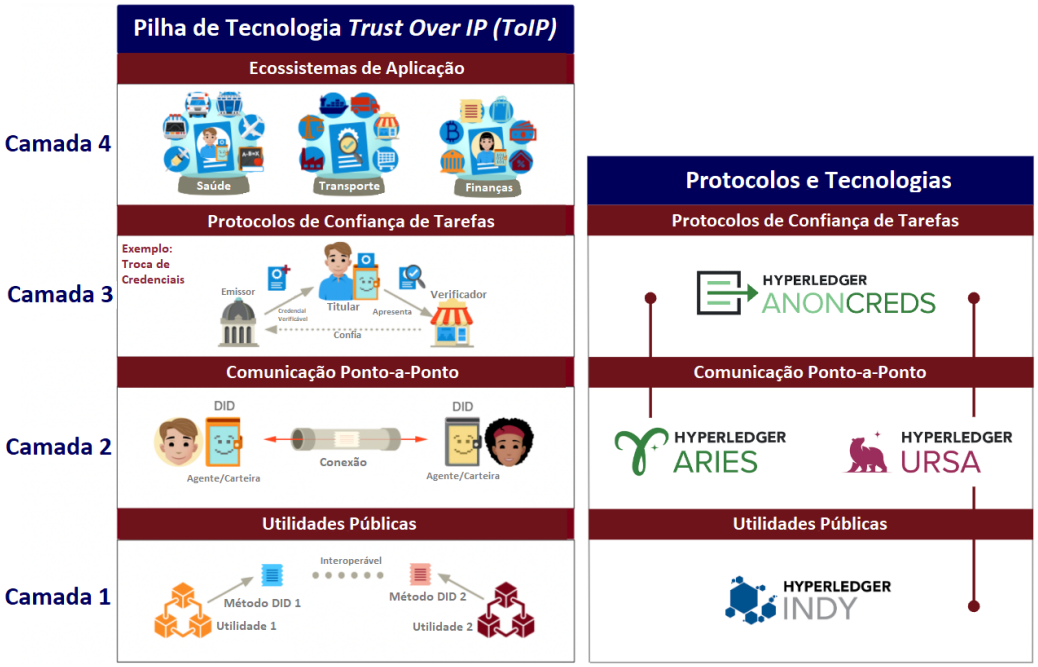

Figura 2. Pilha de protocolos para identidades descentralizadas da Hyperledger (baseada em imagem de [4]).

RESULTADOS E DISCUSSÕES

De forma a melhor entender os custos e a aceitação da autenticação baseada em SSI, propomos neste trabalho uma combinação desta tecnologia com o método tradicional de autenticação federada nas plataformas da Comunidade Acadêmica Federada (CAFe) da RNP. Assim, apresentamos uma proposta híbrida temporária, a qual permite que os usuários tenham a liberdade de escolher entre autenticar-se utilizando o método tradicional, com usuário e senha ou optar pela autenticação via SSI.

Nessa proposta, o fluxo de autenticação atual na plataforma CAFe, conforme representado na Figura 3, permanece inalterado até o passo 5. A partir desse ponto, introduzimos um novo processo que oferece ao usuário a possibilidade de se autenticar por meio de Identificadores Descentralizados (DID),

como pode ser visto na Figura 4. Ao adicionar novos fluxos de comunicação entre o usuário e o IdP, permitimos que o usuário faça sua escolha de autenticação. Notavelmente, as mudanças são focadas exclusivamente nos IdPs, preservando a infraestrutura e comunicações já estabelecidas dentro do ambiente da RNP. Dessa forma, a experiência dos usuários com os serviços da RNP permanece consistente e sem interrupções.

Para viabilizar a autenticação via SSI, um servidor auxiliar é introduzido na instituição do usuário. Após a verificação bem-sucedida das credenciais, esse servidor repassa as informações sobre o usuário para o IdP, que transmite as informações nos protocolos e formatos já conhecidos pelos serviços, garantindo uma transição transparente.

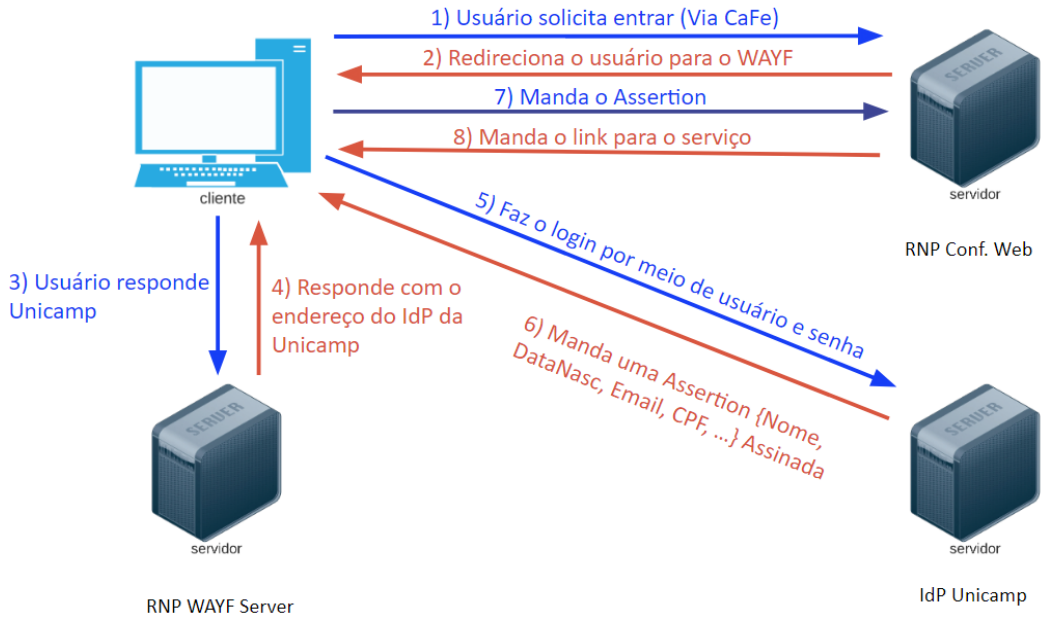

Figura 3. Fluxo de autenticação na federação CAFe.

Com essa solução, a Federação CAFe da RNP estará preparada para uma transição mais suave para a autenticação SSI, permitindo que os usuários desfrutem dos benefícios dessa tecnologia avançada de forma opcional, ao mesmo tempo que fornecem dados para análises sobre custos, viabilidade e aceitação desse novo método de autenticação.

A fim de alcançar com êxito os objetivos propostos buscamos uma abordagem colaborativa e estabelecemos contato com o laboratório de Gestão de Identidades da RNP (GIDLab), cujo apoio tem sido fundamental para o avanço do projeto. Através dessa parceria, foi disponibilizado um ambiente de testes especializado, o que nos permite realizar a implementação da ponte entre o autenticador SSI e o IdP de forma controlada e segura. Essa colaboração com a GIDLab assegura que possamos conduzir experimentos e ajustes necessários, garantindo que a transição para a autenticação via SSI seja realizada de maneira praticamente idêntica àquela usada pela comunidade acadêmica.

Outra discussão importante é sobre a relação custo/benefício de tal implementação. A abordagem descrita permite ter uma avaliação dos benefícios e uma ideia inicial dos custos. Embora não seja obrigatório utilizar blockchains para fornecer o suporte distribuído necessário ao SSI, é importante notar que a crescente disseminação dessa tecnologia facilita sua adoção e reduz os custos de operação. O ambiente Hyperledger permite que se crie uma blockchain exclusiva para a aplicação (plataforma Indy), o que gera custos de implantação e manutenção. Outra opção é utilizar uma blockchain já consolidada, trazendo custos para criação de novos DIDs. A RNP tem projeto em andamento para a criação de um blockchain acadêmica e será necessária uma análise aprofundada dessa alternativa para se conhecer melhor a relação custo/benefício da adoção de autenticação SSI na rede nacional de ensino e pesquisa.

CONCLUSÕES

O novo modelo de autenticação baseado em SSI promete trazer vantagens, mas também custos e dificuldades. Uma transição suave da autenticação tradicional para a autenticação via SSI nas plataformas da Federação CAFe está sendo buscada no ambiente de testes do GIDLab. Entretanto, os próximos passos para a obtenção do resultado final envolvem a realização de mais testes e implementação de um projeto piloto em escala reduzida. Com essas etapas, buscamos avaliar a viabilidade, aceitação e sucesso da autenticação via SSI ao proporcionar uma experiência de autenticação alternativa para toda a Federação CAFe.

Nesse contexto, a análise de custo/benefício desempenha um papel fundamental na determinação da melhor abordagem para a implementação da autenticação via SSI na RNP. A escolha entre criar uma blockchain exclusiva para a aplicação ou utilizar outra já existente envolve considerações sobre os custos associados a cada opção, como os gastos contínuos para manter a blockchain atualizada e disponível no caso do Hyperledger Indy, ou os custos adicionais na criação de novos DIDs ao utilizar outra blockchain. Com a implantação de uma blockchain acadêmica na RNP, será possível fazer uma avaliação mais aprofundada e determinar a viabilidade da transição para a autenticação via SSI na comunidade acadêmica suportada pela RNP.

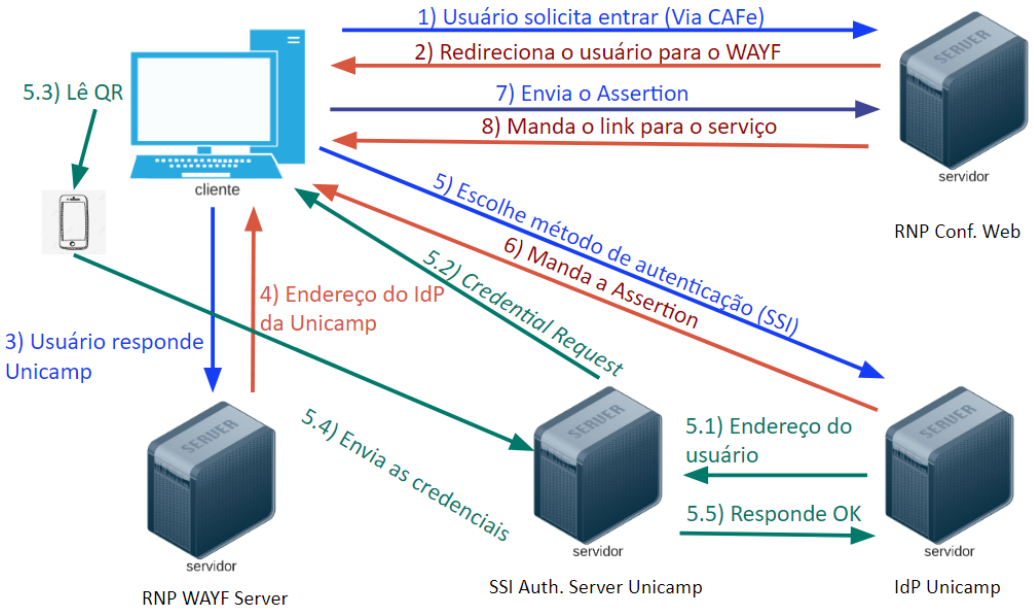

Figura 4. Novo fluxo de autenticação via DID (caso de sucesso na verificação).

BIBLIOGRAFIA

[1] REED, Drummond et al. Decentralized Identifiers (DIDs) v1.0 - **Core architecture, data model, and representations.** W3C Working Draft, Março 2021. Disponível em: https://www.w3.org/TR/2021/WD-did-core-20210309.

[2] TOTH, K. C.; ANDERSON-PRIDDY, A. **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.

[3] FERDOUS, M. S. et al. **In Search of Self-Sovereign Identity Leveraging Blockchain Technology.** In: IEEE Access, vol. 7, pp. 103059-103079, 2019. DOI: 10.1109/ACCESS.2019.2931173.

[4] LINUX FOUNDATION. **Introduction to Hyperledger Self-Sovereign Identity Blockchain Solutions.** Disponível em: https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS172x+1T2023/home.