Um estudo preliminar sobre a criação de autenticação alternativa via identificadores descentralizados Aries para a Federação CAFe da RNP

Giovanni M. Quintella Gama **Marco A. Amaral Henriques**

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

g247122@dac.unicamp.br marco@dca.fee.unicamp.br

Abstract. *Self-Sovereign Identity (SSI) is a novel model for digital identity management that aims to provide users with absolute and exclusive control over their data, which is currently centralized in the hands of third parties. In this work, we present an analysis and experimental evaluations of the Hyperledger Aries SSI solution, with the objective of assessing its potential as an authentication alternative in the CAFe Federation of RNP.*

Resumo. *A Identidade Autossoberana (SSI) é um novo modelo de gerenciamento de identidades digitais, que busca oferecer aos usuários o controle absoluto e exclusivo de seus dados, atualmente centralizados nas mãos de terceiros. Neste trabalho, apresentamos uma análise e algumas experimentações sobre a solução de SSI Hyperledger Aries, com o objetivo de avaliar o seu potencial como alternativa de autenticação na Federação CAFe da RNP.*

1. Introdução

Quando interagimos no mundo físico, frequentemente precisamos fornecer informações pessoais. Esse ato implica na apresentação de evidências próprias, que garantem a autenticidade das informações fornecidas [Johnson, 2008]. No contexto digital, o mecanismo fundamental para estabelecer a identidade de uma pessoa é a combinação de um nome de usuário e uma senha, que são criados em cada serviço *online*. No entanto, surgem desafios nesse cenário: a dificuldade de gerenciar múltiplas senhas, a vulnerabilidade de senhas fracas a ataques digitais e o risco associado ao uso de senhas idênticas em diversos serviços.

Atualmente uma abordagem comum para mitigar esses problemas envolve o uso de provedores de identidade (IdPs - *Identity Providers*), como o *Facebook* ou o *Google*. Nesse modelo, sites e serviços menores utilizam tais IdPs para autenticação e obtenção de informações básicas, como nome e endereço de e-mail. No entanto, essa abordagem tem suas limitações, pois cada uso de um IdP resulta na coleta de informações do usuário, comprometendo a privacidade e permitindo a monetização dos dados por terceiros.

Este estudo explora o potencial do Hyperledger Aries, uma solução de Identidade Autossoberana (SSI), como alternativa de autenticação por IdPs. A Federação CAFe da RNP é usada como caso de estudo. O objetivo é disponibilizar a autenticação SSI baseada em Identificadores Descentralizados (DIDs) nesse contexto acadêmico federado, permitindo que os usuários avaliem e escolham entre o método tradicional e o de SSI, o qual oferece aos usuários controle absoluto sobre seus dados, eliminando a necessidade de confiar em terceiros para a gestão de identidades [Kshetri, 2019].

O restante deste artigo está organizado em cinco seções. A seção 2 descreve as SSIs, incluindo os conceitos de Credenciais Verificáveis (CVs). A seção 3 aborda os Fluxos de Verificação de Identidade, propondo uma transição da autenticação tradicional para a autenticação SSI na CAFe. A seção 4 discute os detalhes da implementação, incluindo a criação de uma ponte S2SB (SAML to SSI Bridge) para integrar o SSI na CAFe. Finalmente, a seção 5 apresenta as conclusões, ressaltando os benefícios e desafios associados à adoção da SSI em tal federação, enfatizando a importância da segurança do usuário nesse contexto.

2. Identidades Autossoberanas

No meio cibernético, Credenciais Verificáveis (CVs) são atributos assinados criptograficamente por autoridades e utilizados para comprovar alguma informação sobre seus titulares. O uso de certificados digitais pelos emissores torna as CVs muito úteis no ambiente *online*, pois o titular não está autoafirmando os seus dados e tampouco pode forjar a criptografia da autoridade. Assim, as CVs podem ser legitimadas, desde que o verificador comprove a assinatura do emissor das mesmas.

No modelo SSI, os dados são entregues ao (e controlados pelo) seu titular, que é quem decide quando e como eles serão compartilhados com terceiros e, se forem compartilhados, até quando isso deve ser feito. Em SSI não há a presença de uma autoridade central que mantenha todas as informações e as repasse a outros quando requisitada.

Segundo [Reed et al., 2021], DID é um identificador que viabiliza identidades digitais descentralizadas verificáveis, podendo identificar pessoas, organizações, entidades abstratas etc. São projetados para serem independentes de registradores centralizados, IdPs e autoridades certificadoras. Ainda existem terceiros que auxiliam no processo de localização das informações relacionadas aos DIDs, mas seu detentor deve ser capaz de provar o controle sobre eles usando técnicas criptográficas ou algum outro método de verificação sem requerer permissão ou depender de terceiros [DID Working Group, 2022].

Um esquema de SSI possui características essenciais, incluindo gestão centrada no usuário, interoperabilidade, controle do usuário sobre a divulgação de identificadores, facilidade de uso em diferentes sites e autonomia do usuário. Além disso, permite que o usuário agregue alegações confirmadas por terceiros, aumentando a confiabilidade da identidade digital [Toth and Anderson-Priddy, 2019]. A Fig. 1 mostra um fluxo de emissão e verificação de CVs.

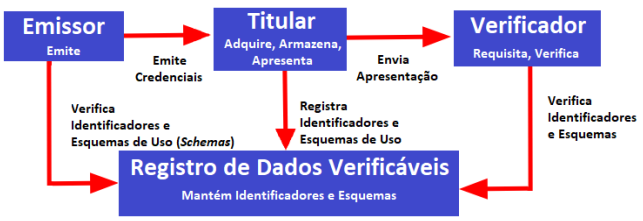

Figura 1. Representação do modelo de *SSI* e seus principais atores

É possível comparar uma CV a um certificado pessoal integrado com Blockchain, destacando-se a SSI/CV por sua abordagem descentralizada. Nela, os usuários mantêm posse exclusiva de suas credenciais e decidem como compartilhá-las.

Em contraste, os certificados pessoais descentralizados com Blockchain ainda exigem uma entidade central para emissão e gerenciamento, trazendo os problemas da centralização.

No que diz respeito à segurança, a SSI introduz uma camada adicional de proteção, tornando o roubo de credenciais mais difícil. Os DIDs e os protocolos criptográficos subjacentes garantem a integridade das credenciais e a autenticidade do usuário. Embora desafios técnicos e de integração sejam esperados na implementação da SSI na Federação CAFe, acreditamos que as vantagens em termos de segurança e privacidade superam os obstáculos. No entanto, é essencial estar ciente de possíveis ameaças e ataques, como a falsificação de DIDs ou ataques de phishing direcionados a usuários. A mitigação desses riscos requer uma abordagem holística, incluindo conscientização e treinamento dos usuários, além de outras medidas.

Diversas iniciativas visam desenvolver sistemas de gestão de identidades descentralizadas, frequentemente incorporando tecnologias de blockchain devido à descentralização, alta disponibilidade e imutabilidade que oferecem. Entre as soluções analisadas por Ferdous et al. [Ferdous et al., 2019], destacam-se *uPort/Serto*, *Blockcerts*, *Jolocom* e *Sovrin Hyperledger*.

O Projeto *Hyperledger* entrou no cenário da gestão de identidades em 2017 com a criação da *Indy*, o primeiro *framework* totalmente dedicado à gestão de identidades. Ao longo do tempo, várias camadas foram desenvolvidas e separadas para oferecer maior flexibilidade nas aplicações. Surgiram o *Ursa*, centrado em criptografia; o *AnonCreds*, um mecanismo de CVs baseado em *Zero Knowledge Proof*; o *Indy*, uma aplicação de blockchain pública e permissionada projetada para casos de uso de identidade descentralizada; e o *Aries*, responsável pelos agentes dentro do *Hyperledger*. Em conjunto, essas camadas compõem a *Hyperledger Identity Stack*, apresentada na Figura 2, que tem como característica principal a sua flexibilidade, permitindo integração com diferentes soluções de camadas 1, 2 e 3.

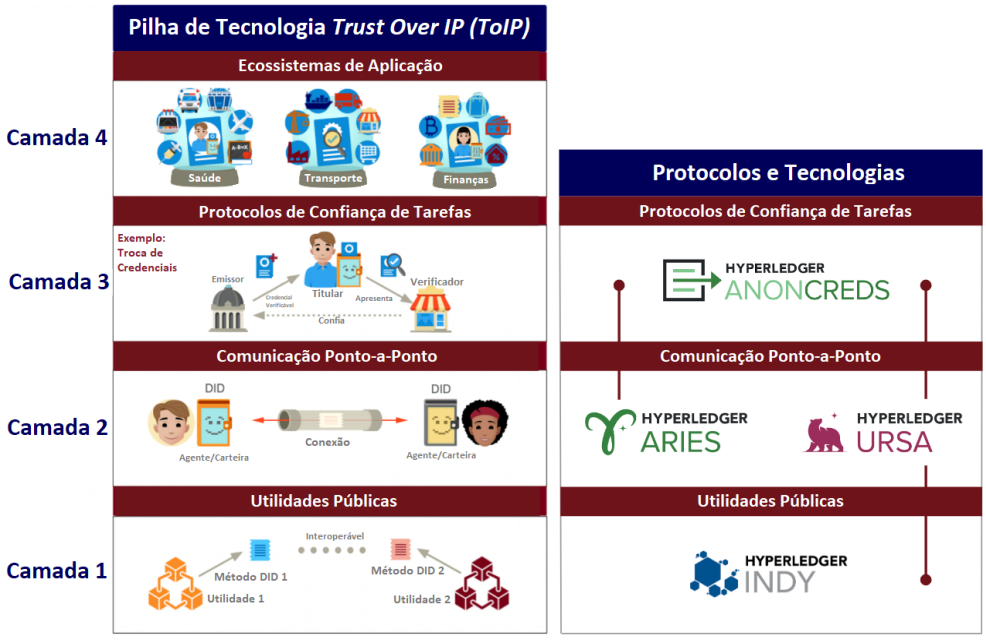

Figura 2. Pilha de protocolos para identidades descentralizadas da *Hyperledger*

(baseada em imagem do curso "*Introduction to Hyperledger Self-Sovereign Identity Blockchain Solutions*", *Linux Foundation*).

3. Fluxos de verificação de identidade

Um dos objetivos é facilitar a transição do método de autenticação tradicional nas plataformas da CAFe para SSI. Os usuários, ao serem redirecionados para seus respectivos IdPs, poderiam ter a opção de autenticar-se de maneira tradicional (usuário e senha) ou por CVs. Isso possibilitaria uma transição mais suave e a implementação ou não da autenticação SSI seria opcional para cada IdP, permitindo coleta de opiniões e uma análise da viabilidade e aceitação desse novo método.

3.1. Fluxo atual para uso dos serviços da RNP

Um fluxograma que representa um resumo da autenticação atual na plataforma CAFe pode ser encontrado na Figura 3 (fluxos com numeração simples de 1 a 8 em azul e vermelho). O usuário solicita algum serviço e, após se comunicar com o servidor, é redirecionado pelo serviço WAYF (*Where Are You From)* para seu respectivo IdP, que faz sua autenticação e responde com uma asserção de segurança, contendo informações sobre o usuário e seus atributos. Isso acarreta na liberação de acesso ao serviço solicitado.

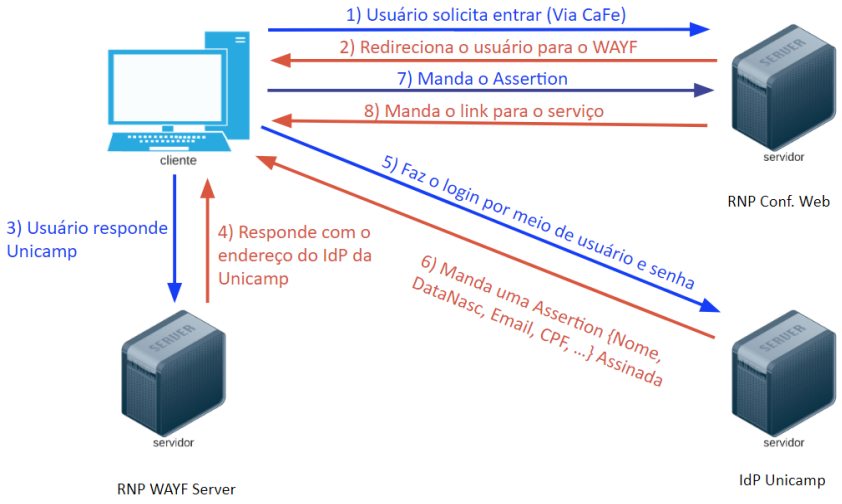

Figura 3. Fluxo de autenticação na federação CAFe.

3.2. Inclusão de fluxo com autenticação via DIDs

Para viabilizar a nova forma de autenticação adicionamos novos fluxos, entre o usuário, o IdP e um serviço externo. A Figura 4 demonstra o caso em que ele se autentica pelo novo método (fluxos verdes de 5.1 a 5.5). Podemos ver que na visão dos servidores da CAFe nada muda. Haverá a adição na instituição do usuário de um servidor auxiliar para autenticar via SSI e, a partir do momento que as credenciais forem validadas, tal servidor encaminha as mesmas para que o IdP as transmita no protocolo e formato já conhecidos pelos serviços.

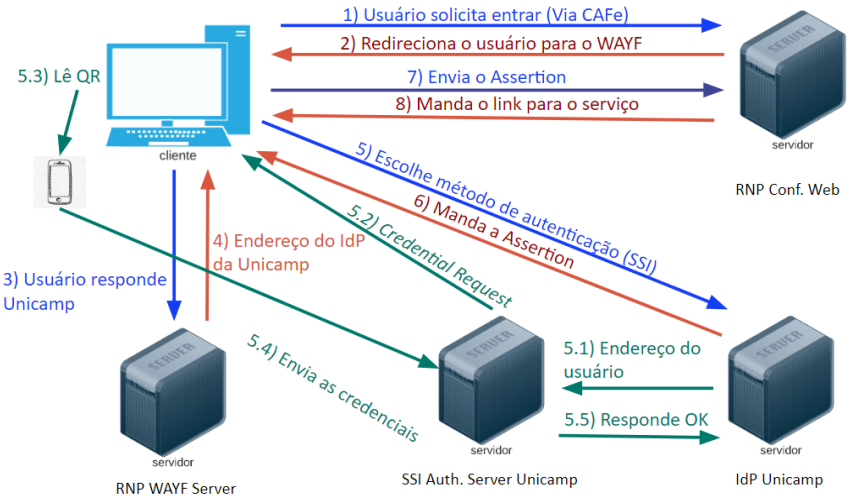

Figura 4. Novo fluxo de autenticação via DID integrado ao fluxo tradicional (caso de sucesso na verificação).

Ao incluir novas comunicações do passo 5 em diante, permitimos que o usuário possa escolher se quer se autenticar por CVs. Assim é possível manter a comunicação já existente dentro da Federação CAFe e fazer pequenas mudanças apenas nos IdPs.

4. Discussão

O Laboratório de Identidades Digitais da RNP (GIDLab) forneceu acesso ao ambiente de testes da CAFe Expresso, que é muito semelhante à federação em produção.

Analisando os fluxos apresentados, percebe-se que o foco principal é implementar uma ponte S2SB (SAML to SSI Bridge) entre o IdP e o servidor de SSI (SSIS) no contexto da CAFe Expresso. Isso permitirá que a autenticação via SSI seja incorporada de maneira gradual e flexível, sem perturbar o funcionamento padrão. Essa abordagem deverá ser baseada em facilidades oferecidas pelas versões recentes de IdP (que aceita a incorporação de um fluxo externo de autenticação) e novas ferramentas como Proxy Satosa e projetos disponíveis como o SP-Django-Python.

O processo S2SB será iniciado pelo IdP, estabelecendo uma conexão com o SSIS. Essa conexão incluirá o endereço e a porta para comunicação com o navegador do usuário. O SSIS solicitará as credenciais e, com base nas informações recebidas da *Wallet*, gerará um sinal de autenticação bem-sucedida (Ok) ou não (Nok). Em seguida, essas credenciais serão enviadas de volta ao IdP, que as incluirá em uma mensagem SAML padrão da federação. Essa mensagem será encaminhada pelo navegador ao Serviço de Provedor original, que receberá as credenciais desejadas sem tomar conhecimento do tipo de autenticação feita.

Apesar de ainda não haver uma discussão sobre que infraestrutura de SSI e que método DID adotar definitivamente, entendemos ser mais simples e prático neste momento adotar o próprio método da *Indy* da plataforma *Hyperledger*.

5. Conclusões

Este estudo discutiu uma forma de viabilizar a implementação da autenticação baseada em SSI na Federação CAFe da RNP. Ainda não foi possível considerar os benefícios e desafios associados devido ao trabalho ainda estar em andamento.

Entretanto, já é possível constatar que a SSI oferecerá aos usuários um maior controle sobre suas informações pessoais, sem a presença de uma autoridade central que mantém todas as informações e as libera quando necessário. Isso não apenas protege a privacidade do usuário, mas também impede a monetização não autorizada de dados pessoais. Também é possível constatar que há maneiras simples e gradativas de se implementar um novo modelo de autenticação baseado em SSI, sem afetar a maior parte dos serviços em produção.

A introdução da SSI na Federação CAFe pode representar um avanço significativo em direção a um sistema de autenticação mais seguro e centrado no usuário. Embora desafios técnicos e de segurança devam ser abordados, os benefícios esperados em termos de privacidade e controle pelo usuário parecem justificar a exploração dessa abordagem inovadora.

Referências

[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

[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.

[Linux Foundation, 2023] “Introduction to Hyperledger Self-Sovereign Identity Blockchain Solutions”, https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS172x+1T2023/home.

[Linux Foundation, 2023] “Becoming a Hyperledger Aries Developer”, https://learning.edx.org/course/course-v1:LinuxFoundationX +LFS173x+1T2023/home

[Johnson, 2008] Johnson, A. (2008). Personal Identity and Authenticity. In Proceedings of the 2008 International Conference on Security & Management (SAM'08) (pp. 262-267).

[Kshetri, 2019] Kshetri, N. (2019). Blockchain’s roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 43(11), 101830. doi: 10.1016/j.telpol.2019.101830.

[DID Working Group, 2022] "Decentralized Identifiers (DIDs) v1.1 - Core architecture, data model, and representations", W3C Working Draft, https://www.w3.org/TR/did-core-2022-07-07/, Julho 2022.