Testbed para Proxies de Gestão de Identidades: Uma Análise Prática do Shibboleth, SimpleSAMLphp e SATOSA

Luan Matheus Trindade Dalmazo[1], Jorge Farias[2], Airton Ribeiro Filho[3]
Luiza Kuze Gomes[4], Maria Amanda de Freitas Morais [5]
Fiterlinge Martins de Sousa[6], Michelle Silva Wangham[7]

[1]Universidade Federal Paraná (UFPR)

[2]Universidade Federal de Pernambuco (UFPE)

[3]Universidade Federal de Viçosa (UFV)

[4]Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC)

[5]Universisdade Federal do Rio Grande do Norte (UFRN)

[6]Rede Nacional de Ensino e Pesquisa (RNP)

[7]Universidade do Vale do Itajaí (Univali)

luantrindade@ufpr.br

jsfj@cin.ufpe.br

airton.r.filho@ufv.br

fiterlinge.sousa@rnp.br

wangham@univali.br

luizakuze08@gmail.com

amanda.morais.110@ufrn.edu.br

Abstract. *Identity Management is a field marked by ongoing discussions, among which the need for tools that enable integration between different communication protocols stands out. In this context, proxies have been widely used to facilitate interoperability between services. This paper presents a platform based on Keycloak designed for experimentation with the main proxies currently in focus: SATOSA, Shibboleth as a SAML proxy, and SimpleSAMLphp. The goal is to provide a testing and evaluation environment for these tools, while also proposing possible usage architectures based on the specific characteristics of each proxy. The results show that proxies can be applied in various scenarios, such as expanding service access to users from federations like CAFe.*

Resumo. *A Gestão de Identidade é uma área marcada por debates recorrentes, entre os quais se destaca a necessidade de ferramentas que viabilizem a integração entre diferentes protocolos de comunicação. Nesse contexto, proxies têm sido amplamente utilizados para facilitar a interoperabilidade entre serviços. Este artigo apresenta uma plataforma baseada em Keycloak voltada à experimentação com os principais proxies em evidência: SATOSA, Shibboleth*

como proxy SAML e SimpleSAMLphp. O objetivo é oferecer um ambiente de testes e avaliação dessas ferramentas, ao mesmo tempo em que propõe possíveis arquiteturas de uso com base nas características de cada proxy. Os resultados demonstram que os proxies podem ser aplicados em diferentes cenários, como a ampliação do acesso a serviços para usuários de federações como a CAFe.

1. Introdução

Com o avanço das aplicações distribuídas, garantir a interoperabilidade tornou-se um desafio central. Entre as soluções mais adotadas estão *middlewares* e, em especial, *proxies*, que conectam componentes heterogêneos sem exigir mudanças profundas em cada sistema. Contudo, essa integração requer, além da simples conectividade, mecanismos de segurança robustos, papel cumprido pela Gestão de Identidades e Acessos (IAM) [Pace 2008].

Como cada sistema costuma apoiar-se em diferentes arquiteturas e tecnologias, o uso de *proxies* viabiliza o diálogo entre sistemas distintos, preservando suas bases originais. A importância desses intermediários na gestão de identidades é detalhada no relatório da *InCommon Federation* [Barton et al. 2023], que descreve os chamados *Federation Proxies*, seus benefícios e desafios, da transparência no uso de atributos do usuário ao gerenciamento de relações federadas. Diante da constante evolução dos navegadores, os requisitos de comunicação entre sistemas evoluem, e os protocolos de comunicação passam por revisões contínuas. Diante da importância desse tema, este artigo apresenta uma análise abrangente de diversos casos de uso de *proxies* no contexto de IAM, com ênfase em sua aplicabilidade, além de mostrar um testbed completo baseado em keycloak com três diferentes próxies e seus respectivos fluxos .

Dentre as principais contribuições deste trabalho, destacam-se, a análise de protocolos que possibilitem a comunicação entre sistemas heterogêneos, como *SAML* e *OpenID Connect*; detalhamento do uso de *proxies* como SimpleSAMLphp, Shibboleth e SATOSA em diferentes contextos de *Single-Sign-On* (SSO), como EntraID, TOPDesk e E-Astronomia, através da sugestão de arquiteturas de uso; disponibilização de uma ferramenta baseada em Keycloak que permite a experimentação das soluções apresentadas; discussão sobre o papel dos *proxies* na superação dos desafios relacionados à interoperabilidade.

2. Trabalhos Relacionados

Na Tabela 1 são apresentados trabalhos relacionados que exploram soluções para a integração de identidades digitais, e uma comparação com a solução proposta nesse trabalho.

3. *Proxies e Casos de uso*

Proxies são intermediários que atuam entre o cliente e o servidor final, facilitando e controlando a comunicação entre esses dois pontos. Eles são amplamente utilizados para aumentar a segurança, gerenciar o tráfego de rede e realizar o *cache* de conteúdos. Já os *Proxy Servers* [Abiona et al. 2014] não apenas desempenham as funções de um *proxy* comum, mas também realizam etapas adicionais internamente ao processar e encaminhar

Tabela 1. Comparação entre trabalhos relacionados e a proposta deste trabalho

Referência	**Contribuição Principal**	**Tecnologia Utilizada**	**Limitações**	**Inovação deste Trabalho**
[Berbecaru et al. 2011]	Extensão do Proxy SAML para suporte a *roaming* com meta-atributos dinâmicos	Proxy SAML (STORK)	Cenário restrito ao acesso sem fio e uso específico de meta-atributos	Ambiente genérico e controlado para avaliação de múltiplos proxies em diferentes cenários
[Vo et al. 2019]	Proposta de IDaaS com foco na privacidade usando OpenID	OpenID Attribute Exchange e recriptografia por proxy	Solução teórica com foco exclusivo em privacidade	Comparação prática entre soluções com foco em aplicabilidade nacional e federativa
[Catuogno and Galdi 2014]	Interoperabilidade entre Shibboleth e PAPI usando ponte de tradução de protocolos	Shibboleth e PAPI	Solução específica para dois sistemas, sem comparação ampla de proxies	Avaliação comparativa e proposta de arquitetura adaptável a múltiplos contextos federativos
Este trabalho	Avaliação e experimentação de proxies de identidade federada	Diversos proxies de identidade federada	–	Ambiente de testes comparativo, apoio à escolha arquitetural e incentivo à adoção de identidades federadas

solicitações. Esse processo contribui para proteger a identidade e os dados dos clientes, além de oferecer funcionalidades extras.

Nos sistemas de gestão de identidades, os *Proxy Servers* são fundamentais para facilitar a integração entre diferentes provedores de identidade e provedores de serviços. Eles desempenham o papel de mediadores em solicitações de autenticação e autorização, garantindo que sistemas, protocolos e serviços distintos possam se comunicar de forma eficiente e segura.

Sistemas podem diferir quanto ao uso de protocolos variando entre SAML, OAuth2 e OIDC, para este caso, ferramentas como *Shibboleth* como *proxy* SAML, SimpleSAMLphp e SATOSA podem ser soluções eficazes ao integrar o fluxo de autenticação, oferecendo interoperabilidade e segurança para os membros da arquitetura. Esta seção tem como objetivo detalhar os *proxies* mais comumente utilizados, além de apresentar casos de uso baseados na aplicação dessas ferramentas.

3.1. *Shibboleth* e *Microsoft Entra ID*

O *Shibboleth*, além de atuar como um IdP ou SP, também pode ser utilizado como *proxy* SAML. Nessa função, constitui uma solução consolidada para cenários em que é necessária a interoperabilidade entre diferentes *frameworks* [Scott Cantor 2012]. Como *proxy*, o Shibboleth opera simultaneamente como IdP para os SPs e como SP para os IdPs, integrando as funcionalidades de ambos. Essa capacidade permite a comunicação entre sistemas distintos baseados em SAML, proporcionando benefícios como maior eficiência,

segurança e flexibilidade nos processos de autenticação e autorização.

O Microsoft Entra ID[1] é uma solução voltada para o gerenciamento de identidades, que facilita a integração e a segurança na comunicação entre diferentes aplicativos e usuários, de modo que ao mesmo tempo oferece funcionalidades de *Single Sign-On*.

Em extensão as possibilidades de uso da plataforma, o Entra ID pode ser utilizado em conjunto com o *Shibboleth*. Nessa configuração, a plataforma da *Microsoft* atua como um IdP, enquanto o *Shibboleth* age como um *Proxy* SAML. Essa abordagem possibilita o uso de fluxos SAML em ambientes de nuvem, ampliando o escopo de aplicação em uma federação. Com isso, entidades integradas ao *Entra ID*, como estudantes e plataformas diversas, podem interagir com uma federação baseada em SAML.

3.1.1. Caso de uso

A Universidade do Estado de Minas Gerais (UEMG) buscava implementar a autenticação federada de usuários no ambiente *Microsoft Entra ID* dentro da federação CAFe da Rede Nacional de Ensino e Pesquisa (RNP), utilizando o protocolo SAML. No entanto, a plataforma *Entra ID* não oferece suporte nativo para federação multilateral. Na prática, os usuários de uma instituição registrados no *Entra Id* não podem ser utilizados por exemplo na *eduGAIN*, na *GÉANT* ou CAFe. Para superar essa limitação, a *Microsoft* propõe três soluções alternativas: o uso do *Entra ID* com a *Ponte do Cirrus*, o *Entra ID* com o *Shibboleth* atuando como *proxy* SAML ou o *Entra ID* integrado ao *AD FS* e ao *Shibboleth*.

Após uma análise detalhada, a universidade escolheu a segunda alternativa, que utiliza o *Shibboleth* como *proxy* SAML. Essa opção foi considerada a mais viável, pois não geraria custos adicionais com *software* para sua implementação.

O *Shibboleth* como *proxy* realiza a mediação da autenticação entre o Entra ID e a CAFe. Esta configuração proporciona uma integração dos sistemas de autenticação, atendendo às necessidades da UEMG. Os testes realizados validaram a proposta, demonstrando que o fluxo de autenticação completo funciona conforme o esperado, evidenciando a viabilidade da solução escolhida. A Figura 1 ilustra a arquitetura desenvolvida para este caso de uso. Neste cenário, o provedor de serviços é o Periódico CAPES, e, por meio da intermediação do IdP Shibboleth, o usuário pode utilizar o *Microsoft* Entra ID como método de autenticação. É importante destacar que a arquitetura proposta pode atender diferentes entidades, considerando que a CAFe é uma das maiores federações acadêmicas do mundo [RNPMais sd] e conta com a adesão de diversas instituições.

Figura 1. Arquitetura utilizada no caso de uso da UEMG.

[1]https://www.microsoft.com/pt-br/security/business/identity-access/microsoft-entra-id

3.2. SimpleSAMLphp

O SimpleSAMLphp (SSP) é uma aplicação de código aberto que possibilita múltiplos usos dentro da temática de gestão de identidades, como o uso como provedor de identidades ou de serviços [SimpleSAMLphp sd]. A aplicação é escrita em PHP e é flexível, dado a possibilidade de utilização de módulos externos propostos pela comunidade, como visto em módulos que lidam com protocolo OIDC[2] ou OAuth2[3], de maneira a ampliar o uso da aplicação para diferentes contextos.

O proxy do SSP funciona da seguinte maneira: o provedor de serviços estabelece uma relação de confiança com o IdP SimpleSAMLphp, trocando metadados entre eles. Quando o SP acessa o IdP, o SSP geralmente redireciona para um sistema de descoberta que oferece diversas opções de IdPs. Esse processo ocorre porque o IdP SSP utiliza um SP interno como fonte autenticadora, o que possibilita a comunicação com outros IdPs. Assim, quando um SP externo permite apenas a comunicação 1 a 1, ou seja, sem aceitar múltiplos IdPs, a inclusão de um IdP SSP amplia as opções de autenticação.

3.2.1. Caso de uso

O TOPDesk[4] é uma ferramenta de gerenciamento de *tickets*, utilizada neste caso para gerenciar e acompanhar os chamados da RNP. Para fins de praticidade, a ferramenta oferece a funcionalidade de login único através de SSO. O objetivo, então, era integrar a ferramenta a federação CAFe, possibilitando a autenticação federada.

O TOPDesk possui dois portais de acesso: autoatendimento e operação. O primeiro é dedicado aos usuários que solicitam os chamados, e o segundo, aos operadores responsáveis pelo atendimento. Cada portal é um provedor de serviço, e para que o SSO seja viabilizado, é necessário estabelecer uma relação de confiança entre cada SP e um IdP, ou seja, apenas uma relação um-para-um. Dessa forma, não é possível integrar um serviço de descoberta ou a inserção de vários provedores de identidade automaticamente.

Para resolver essa limitação, o *proxy* SimpleSAMLphp foi utilizado como solução. Utilizando esse *proxy*, foi possível incorporar um serviço de descoberta, no caso, o WAYF (Where Are You From). Além disso, com o SSP, é possível adicionar IdPs de maneira automática, eliminando a necessidade antiga de inserção manual de cada IdP. Em vez disso, uma única configuração de um IdP do *proxy* é suficiente para cada portal. A Figura 2 apresenta a arquitetura desenvolvida para este caso de uso, na qual o *proxy* SimpleSAMLphp atua como intermediário entre os provedores de serviço do TOPdesk e um provedor de identidade SAML.

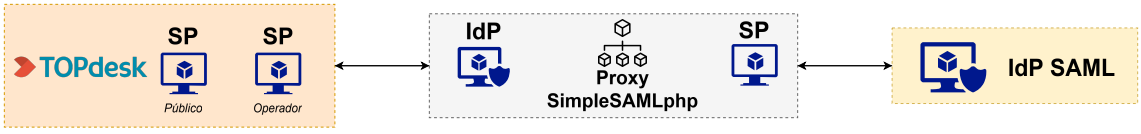

Figura 2. Arquitetura utilizada no caso de uso do TopDesk.

[2]https://github.com/simplesamlphp/simplesamlphp-module-oidc
[3]https://github.com/cirrusidentity/simplesamlphp-module-authoauth2
[4]https://www.topdesk.com/en/

3.2.2. SATOSA

O SATOSA é uma ferramenta de *proxy* para autenticação e autorização [IdentityPython sd]. Suas principais funcionalidades incluem roteamento que direciona solicitações entre IdPs e SPs, transformação de atributos conforme as necessidades de gestão de identidade e extensibilidade por meio de plugins personalizados, além do suporte a múltiplos protocolos de autenticação e autorização, como SAML, OIDC e OAuth2.

3.2.3. Caso de uso

O Linea, Laboratório Interinstitucional de e-Astronomia, é uma organização dedicada ao desenvolvimento de ferramentas e serviços para a astronomia, com foco em projetos de grande escala. Ele promove a colaboração científica e tecnológica entre diversas instituições, visando otimizar a coleta, processamento e análise de dados astronômicos.

Os objetivos deste estudo de caso eram prover o acesso aos serviços do Linea, ofertados para a comunidade acadêmica e pesquisadores autônomos, pela CAFe e por logins sociais, além de centralizar a oferta de múltiplos serviços em uma única plataforma. Dessa forma, o acesso dos usuários é facilitado, garantindo uma gestão mais eficiente e integrada dos recursos disponíveis.

Para esse estudo de caso foi utilizado o SATOSA para realizar a integração dos serviços ofertados no Linea aceitando usuários da CAFe e do Google. Os serviços internos do Linea, é utilizado o SAML. E as fontes de identidades são em SAML quando autenticado pela CAFe, e OpenID Connect (OIDC) quando autenticados pelo Google. A arquitetura utilizada para este caso de uso é ilustrada na Figura 3, na qual os serviços do LIneA (*Science Portal*, *JupyterHub*, *COmanage*) utilizam o *proxy* SATOSA, permitindo a autenticação por meio de um IdP SAML ou logins sociais.

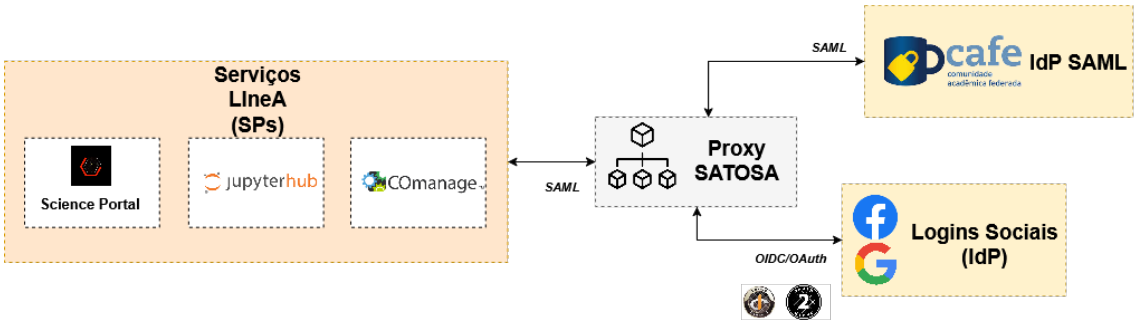

Figura 3. Arquitetura utilizada no caso de uso do LIneA.

Outro estudo de caso com o SATOSA é o da Escola Superior de Redes (ESR). A ESR é uma iniciativa da RNP que oferece cursos de capacitação e desenvolvimento profissional em áreas como redes de computadores, segurança da informação, e gestão de TI. O objetivo do estudo era viabilizar a autenticação de usuários da Federação CAFe, que opera com SAML, em um provedor de serviços que utiliza o protocolo OIDC. Isso possibilita que os usuários da CAFe acessem serviços modernos que adotam OIDC, integrando dois ecossistemas de autenticação diferentes.

4. Plataforma para experimentação de *proxies* baseada em Keycloak

Embora o uso de *proxies* seja indispensável em situações específicas, sua configuração e implementação podem demandar um tempo considerável, especialmente em cenários de desenvolvimento. Para facilitar a avaliação e promover um ambiente de testes para as abordagens discutidas nas seções anteriores, propõe-se a criação de um ambiente experimental baseado no *Keycloak*, uma plataforma de código aberto voltada para o gerenciamento de identidades [Keycloak sd]. A Figura 4 apresenta a arquitetura do ambiente proposto, onde o *Keycloak* atua como um concentrador, simulando os serviços *TOPdesk*, LIneA e Periódico CAPES, e garantindo o acesso a eles por meio dos *proxies* Shibboleth, SATOSA ou SimpleSAMLphp. A documentação do ambiente está presente neste repositório[5], os vídeos explicativos nessa pasta e a plataforma pode ser utilizada no seguinte link: Plataforma para experimentação de proxies [6].

Na documentação fornecida, são disponibilizadas credenciais para acesso e testes dos *proxies*. Todas as ferramentas foram configuradas para funcionar como um *toy example*, com o objetivo de verificar seu funcionamento e observar como informações, como atributos do usuário, são transmitidas entre protocolos com padrões distintos. Ao fim do processo, são exibidos os dados do usuário que realizou o *login*.

O ambiente funciona como um *playground*, e suas funcionalidades podem ser integradas a outras aplicações que demandem o intercâmbio de informações de usuário entre diferentes serviços. Até onde se sabe, esta é a primeira plataforma a propor esse tipo de experimentação, e as documentações de cada *proxy*, de forma individual, viabilizam a reprodutibilidade tanto do ambiente completo quanto das ferramentas isoladamente.

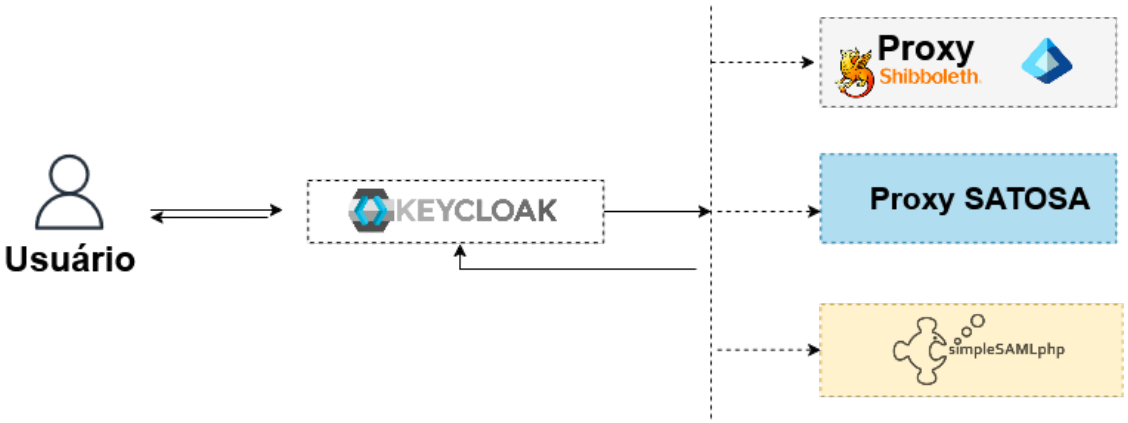

Figura 4. Fluxo de degustação proposto.

4.1. Planejamento para demonstração

Para a demonstração da ferramenta, é suficiente a disponibilização de uma máquina com acesso à Internet e um monitor. Todos os *proxies* foram previamente configurados e estão acessíveis publicamente, de modo que não há necessidade de reconfiguração para fins de experimentação.

[5]https://github.com/luandalmazo/tools
[6]https://keycloak.gidlab.rnp.br/

Durante a demonstração, será apresentada uma plataforma prática desenvolvida com base no Keycloak, que permite a experimentação com os principais proxies de identidade atualmente em evidência: Shibboleth (como proxy SAML), SimpleSAMLphp e SATOSA. A plataforma foi projetada para simular cenários reais de integração entre serviços e federações acadêmicas, como a CAFe, possibilitando avaliar o comportamento e a compatibilidade de cada proxy em diferentes arquiteturas.

O foco principal da demonstração é garantir a reprodutibilidade dos experimentos realizados. Para isso, serão exibidas as configurações completas dos três proxies, bem como a estrutura do ambiente de testes utilizado. Os participantes poderão visualizar arquiteturas típicas de uso, fluxos de autenticação e as etapas necessárias para replicar os cenários apresentados em seus próprios contextos institucionais.

Essa abordagem oferece uma base sólida para instituições que desejam ampliar o acesso a serviços via federações ou modernizar suas infraestruturas de autenticação, ao mesmo tempo em que promove transparência e facilidade na adoção das soluções demonstradas.

5. Conclusão

Ao longo deste artigo, foram analisadas três soluções de *proxies* de gestão de identidade, com destaque para suas funcionalidades, benefícios e desafios na promoção da interoperabilidade entre sistemas. Esses intermediários têm papel central na gestão segura e eficiente de informações, especialmente diante da evolução dos protocolos e da crescente demanda por integração. Ainda persistem desafios como a conformidade de políticas entre IdPs e SPs, e a transparência no fluxo de autenticação, principalmente quanto aos atributos de usuário e aos agentes envolvidos. Espera-se que este trabalho contribua tanto para a avaliação de diferentes *proxies* quanto para o enfrentamento desses obstáculos.

Referências

Abiona, O., Oluwaranti, A., Oluwatope, A., Bello, S., Onime, C., Sanni, M., and Kehinde, L. (2014). Proxy server experiment and network security with changing nature of the web. *International Journal of Communications, Network and System Sciences*, 7(12):519–528.

Barton, T., Klingenstein, K., Rank, M., Walker, D., and Albert, W. (2023). Formalizing the role of federation proxies within the incommon federation.

Berbecaru, D., Lioy, A., and Aime, M. D. (2011). Exploiting proxy-based federated identity management in wireless roaming access. In *Trust, Privacy and Security in Digital Business: 8th International Conference, TrustBus 2011, Toulouse, France, August 29-September 2, 2011. Proceedings 8*, pages 13–23. Springer.

Catuogno, L. and Galdi, C. (2014). Achieving interoperability between federated identity management systems: A case of study. *Journal of High Speed Networks*, 20(4):209–221.

IdentityPython (s.d.). *SATOSA*. Acessado em: 08 fev. 2025.

Keycloak (s.d.). *Keycloak*. Acessado em: 08 fev. 2025.

Pace, A. (2008). Identity management. 119(1):012002.

RNPMais (s.d.). Comunidade Acadêmica Federada (CAFe) - RNP+. `https://rnpmais.rnp.br/comunidade-academica-federada-cafe`. Acesso em: 12 maio 2025.

Scott Cantor (2012). *SAMLIdPProxy*. Acessado em: 08 fev. 2025.

SimpleSAMLphp (s.d.). *SimpleSAMLphp Documentation*. Acessado em: 08 fev. 2025.

Vo, T. H., Fuhrmann, W., Fischer-Hellmann, K.-P., and Furnell, S. (2019). Identity-as-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. *Future Internet*, 11(5).