Federação SAML no GIdLab: Explorando o Potencial do SimpleSAMLphp para Experimentação

Luan Matheus Trindade Dalmazo[1], Jorge Soares[3], Fiterlinge Sousa[5], Airton Ribeiro Filho[4], Michelle Silva Wangham[2,5]

[1]Universidade Federal do Paraná (UFPR) – Curitiba, PR – Brasil

[2]Universidade do Vale do Itajaí (UNIVALI) – São José, SC – Brasil

[3]Universidade Federal de Pernambuco (UFPE) – Recife, PE – Brasil

[4]Universidade Federal de Viçosa (UFV) – Viçosa, MG – Brasil

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

luantrindade@ufpr.br, jsfj@cin.ufpe.br, fiterlinge.sousa@rnp.br,

airton.r.filho@ufv.br, wangham@univali.br

Resumo. *0 SimpleSAMLphp (SSP) é um framework de código aberto para a implementação de autenticação federada em ambientes web, podendo atuar como provedor de serviços, de identidade ou como proxy. Assim como o Shibboleth, a solução implementa o padrão SAML 2 e é amplamente utilizada em federações acadêmicas. Este trabalho apresenta uma nova federação SAML, baseada no SSP e outros componentes, que segue a mesma arquitetura mesh da Federação CAFe Expresso, porém, utiliza em seu núcleo as ferramentas PyFF (como agregador de metadados) e Thiss.io (como serviço de descoberta). Além disso, a federação possui um Proxy SAML para integração com a Federação CAFe Expresso e um IdP configurado como OpenId Connect provider. Disponibilizada no serviço GIdLab da RNP, esta federação oferece uma nova abordagem para experimentações na área.*

1. Introdução

A gestão de identidade e de acesso (*Identity and Access Management - IAM*) engloba políticas, processos e tecnologias que viabilizam a autenticação e autorização de indivíduos antes e durante transações online [de Mello et al. 2022]. Uma ampla gama de ferramentas pode ser empregada para assegurar a gestão de identidade. Entre as alternativas disponíveis, ganham destaque o SimpleSAMLphp e o Shibboleth, que são soluções que implementam o modelo de identidade federada baseada no protocolo SAML.

O SimpleSAMLphp (SSP) é um *framework* desenvolvido em PHP [Conservancy 2023], similar ao Shibboleth [Consortium 2023], amplamente empregado para habilitar a autenticação web *Single Sign-On*, por meio do protocolo SAML, em federações acadêmicas (por exemplo SIKT na Noruega e SURF na Holanda) e em outros trabalhos [Mateo Sanguino et al. 2018, Andronache e Nisipasiu 2011]. Este framework pode ser adotado em diversas funções, atuando como provedor de identidade (IdP), provedor de serviço (SP) ou até como um proxy intermediário, que opera entre o IdP e o SP. Para além dessas aplicações, o SSP oferece suporte a módulos externos, como o

cronn e o *metarefresh*, ambos voltados para a execução de tarefas em um intervalo de tempo previamente definido.

Tanto o SimpleSAMLphp (SSP) quanto o Shibboleth são empregados para estabelecer federações, que são constituídas por instituições que compartilham atributos e políticas comuns [Wangham et al. 2010]. No núcleo das federações, é comum a utilização de um serviço de descoberta, o qual proporciona uma interface para que um usuário selecione o seu provedor de identidade. Além disso, há o emprego de um agregador de metadados, encarregado de centralizar os metadados das diversas instituições que compõem a federação e com isso estabelecer as relações de confiança.

O objetivo deste trabalho é descrever a construção de uma federação SAML baseada no *framework* SimpleSAMLphp disponível para experimentação no Serviço para Experimentação em Gestão de Identidade da RNP, o GIdLab[1]. Essa federação está fundamentada nas seguintes ferramentas: PyFF como agregador de metadados, Thiss.io como serviço de descoberta e um proxy SSP para integração com a federação CAFe Expresso.

2. Federação SAML baseada no Framework SimpleSAMLphp

Entende-se que uma federação deve possibilitar o intercâmbio seguro de informação entre seus constituintes [Wangham et al. 2010]. Cada entidade pertencente à federação possui metadados que fornecem detalhes sobre suas informações. Consequentemente, tanto um Provedor de Serviços (SP) quanto um Provedor de Identidade (IdP) mantêm um arquivo, frequentemente em formato XML, contendo descritores que abrangem elementos como o nome da instituição, certificados e URLs de acesso, entre outros dados. Em virtude dessa estrutura, ao criar uma nova federação, surge a necessidade de um mecanismo que possibilite a consolidação desses metadados, facilitando a localização de cada entidade. Para atender a essa demanda, é empregado o PyFF.

O PyFF é um agregador de metadados com atributos destacáveis, incluindo funções de validação, combinação e transformação de metadados [Johansson 2012]. Através dessa tecnologia, torna-se viável a inclusão de novos arquivos de metadados, que consequentemente se tornam visíveis para toda a federação. Essa capacidade é frequentemente complementada pelo This.io, uma implementação de um serviço de descoberta de identidade oferecido pela *Coalition for Seamless Access* [Johansson 2019]. Ambas as soluções fazem parte do núcleo da nova federação.

A nova federação SSP é composta por um IdP e um SP Shibboleth, além de um IdP e um SP SimpleSAMLphp para evidenciar que é possível usar os dois frameworks em uma mesma federação. A federação utiliza ainda um *proxy* para permitir que aqueles SPs que são capazes apenas de comunicação *um para um* (isto é, visualizam apenas um IdP e não uma federação), possam utilizar todos os IdPs associados a federação. Por fim, um IdP SSP é configurado como OpenId Connect provider para possibilitar que SPs OpenID Connect (RPs) possam ser utilizados na federação. A Figura 1 ilustra a federação implantada e configurada no Serviço GIDLab.

3. Comparação Federação CAFe Expresso e Federação SSP

A federação CAFe Expresso surgiu para atender as necessidades de pesquisadores que atuam da área de gestão de identidades. Esta oferece IdPs, populados com dados de

[1] `https://www.rnp.br/servicos/testbeds/gidlab`

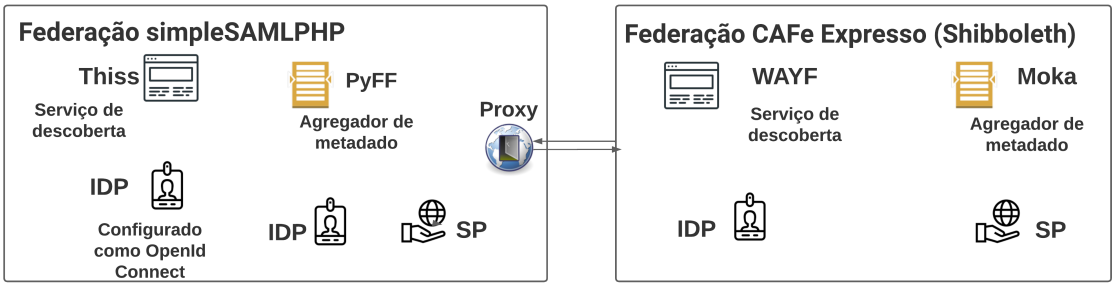

Figura 1. Visão geral da nova federação SAML no Serviço GidLab

usuários fictícios, e SPs aptos a hospedar aplicações web desenvolvidas em PHP, Java ou Python. Com essa estrutura, pesquisadores precisam apenas se preocupar com o desenvolvimento de suas aplicações [Souza et al. 2014]. É necessário entender as diferenças entre a federação CAFe Expresso e a federação SimpleSAMLphp. A Tabela 1 mostra a comparação entre as federações.

Características	**CAFe Expresso**	**Simple Saml PHP**
Serviço de Descoberta	WAYF (Switch)	Thiss.io
Agregador de Metadados	Moka (Serviço proprietário)	PyFF
Inclusão de Federações	Não permite a inclusão da federação SSP	Permite a inclusão da federação CAFe Expresso
SeamlessAccess	Não em conformidade	Em conformidade

Tabela 1. Comparação entre as Federações CAFe Expresso e Simple SAML PHP

As principais diferenças entre as federações estão nas tecnologias utilizadas no núcleo da federação e em algumas características específicas. O agregador de metadados usado na CAFe Expresso não permite adicionar IdPs SSP dentro da federação por questões de incompatibilidade de metadados, já na federação SSP pode-se adicionar todos os componentes da CAFe Expresso e os do framework SSP.

4. Considerações Finais

O Web*Single sign-on* (SSO) garante ao usuário maior dinamicidade no acesso a sua conta [Radha e Reddy 2012]. Quando um modelo federado é utilizado, o acesso é realizado uma única vez através de provedor de identidades distribuídos na federação com o objetivo final de alcançar o provedor de serviços. Com a criação de uma nova federação para experimentação, novos experimentos podem ser conduzidos envolvendo os dois principais *frameworks* que implementam o Web SSO do padrão SAML. A nova federação possibilita ainda a integração com SPs OpenId Connect o que amplias as possibilidades aos pesquisadores e desenvolvedores da área.

Têm-se como perspectiva de trabalhos futuros (i) avaliar uso do MDQ Browser, um serviço de gerenciamento de aplicação ofertado junto ao PyFF, para facilitar a inserção de metadados e disponibilizar rotas para localização de entidades, (ii) implantar o proxy

SATOSA [IdentityPython 2023] e avaliar a integração dessa tecnologia à nova federação e (iii) implantar um solução de monitoramento dos componentes do núcleo da federação e de IdPs e SPs.

A nova federação SAML, baseada em SimpleSAMLphp, amplia o escopo das federações Shibboleth e SSP que eram utilizadas individualmente. Além disso, percebe-se que existem meios para aprimorar ainda mais seu funcionamento, como a utilização de um serviço de monitoramento da plataforma e a integração de outro *proxy*. Portanto, a criação desta nova federação proporciona uma solução robusta e, ao mesmo tempo, abre possibilidades para melhorias adicionais.

Referências

Andronache, I. e Nisipasiu, C. (2011). Web single sign-on implementation using the simplesamlphp application. *Journal of Mobile, Embedded and Distributed Systems*, 3(1):21–29.

Conservancy, T. C. (2023). Simplesamlphp. `https://simplesamlphp.org/`. Acessado em: 2 de agosto de 2023.

Consortium, S. (2023). Shibboleth. `https://www.shibboleth.net/`. Acessado em: 2 de agosto de 2023.

de Mello, E. R., de Chaves, S. A., Da Silva, C., Wangham, M. S., Brito, A., e Henriques, M. A. A. H. (2022). Autenticação e autorização: antigas demandas, novos desafios e tecnologias emergentes. In *Minicurso – SBSeg 2022*.

IdentityPython (2023). SATOSA: A Protocol Proxy for SAML-based Authentication. `https://github.com/IdentityPython/SATOSA`. Acessado em: 07 de agosto de 2023.

Johansson, L. (2012). *pyFF Documentation*. Release 2.0.0.

Johansson, L. (2019). The identity selector software (thiss.io). `https://thiss.io/`. Acessado em: 8 de agosto de 2023.

Mateo Sanguino, T., Fernández Viana González, I., Espejo Fernández, J., e García Domínguez, A. (2018). Using identity provider and automatic resource management to improve a remote networking lab. *IEEE Latin America Transactions*, 16(5):1547–1556.

Radha, V. e Reddy, D. H. (2012). A survey on single sign-on techniques. *Procedia Technology*, 4:134–139. 2nd International Conference on Computer, Communication, Control and Information Technology(C3IT-2012) on February 25 - 26, 2012.

Souza, M., Mello, E., e Wangham, M. (2014). Gidlab: Laboratório de experimentação em gestão de identidade. In *Workshop de Gestão de Identidade (WGID), Anais do XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2014)*, pages 467–468. Sociedade Brasileira de Computação.

Wangham, M. S., de Mello, E. R., da Silva Böger, D., Guerios, M., e da Silva Fraga, J. (2010). Gerenciamento de identidades federadas. In *Minicurso – SBSeg 2010*.