Análise de Soluções de Organizações Virtuais e Relato de Estudos de Caso para Rede de e-Ciência da RNP

Estefânia Arata[1], Bruno José Demborguski[2], Walter Priesnitz Filho[3], Fiterlinge Sousa[1], Reinaldo Gomes[1]

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

[2]Departamento de Ciencia da Computação - UFRRJ

[3]Universidade Federal de Santa Maria (UFSM)

{estefania.arata, fiterlinge.sousa, reinaldo.gomes}@rnp.br,

brunodembogurski@ufrrj.br, walter.filho@ufsm.br

Resumo. *Com o avanço das iniciativas de pesquisa científica junto a grande transferência de dados surgiu a necessidade de analisar soluções de plataformas para proporcionar aos pesquisadores uma maneira de realizar login, com uma única credencial. Diante deste cenário da Rede de e-Ciência duas PoCs foram executadas com objetivo de analisar o CILogon, uma plataforma americana e uma solução baseada no MyAccessID, uma plataforma europeia. Essas soluções são capazes de proporcionar ambientes de organizações virtuais, essenciais para gerenciar todo ciclo de vida entre usuários de diferentes instituições e domínios, garantindo eficiência e segurança.*

1. Introdução

Com o crescimento da colaboração científica entre Instituições de Ciência e Tecnologia (ICTs) distribuídas em diferentes regiões do Brasil e do exterior, surge a necessidade de mecanismos que permitam autenticação e autorização de forma segura e interoperável. Nesse contexto, torna-se essencial disponibilizar aos pesquisadores uma identidade digital única, capaz de viabilizar o acesso aos recursos computacionais, serviços e infraestruturas oferecidos pelas instituições participantes da Rede de e-Ciência.

A Rede de e-Ciência [RNP 2024] consiste em uma infraestrutura digital segura e de alto desempenho, destinada a ICTs que desenvolvem pesquisas intensivas em dados. A infraestrutura oferece conectividade dedicada, com enlaces de alta capacidade, políticas de segurança e serviços especializados para transferência massiva de dados científicos. Seu propósito é apoiar centros de supercomputação, laboratórios multiusuários e demais infraestruturas científicas que demandam elevada capacidade de processamento, armazenamento e compartilhamento de dados, promovendo a colaboração científica nacional.

Para um ambiente que permite compartilhar grande volume de dados e necessita de acesso remoto seguro, se faz necessário o uso de uma identidade digital federada, que seja capaz de gerenciar todo ciclo de vida da Organização Virtual (OV). E ao final de um colaboração, seja possível desprovisionar e revogar os acessos das contas de usuários que não pertencem aquela ICT, garantindo assim que dados não sejam vazados e incidentes de segurança da informação sejam evitados. Para atender a esse cenário, foram estudadas e avaliadas plataformas de Gestão de Identidade Digital capazes de gerenciar o ciclo de

vida dos usuários. A avaliação foi conduzida por meio de Provas de Conceito (PoC), com estudos de caso em duas ICTs participantes da Rede de e-Ciência do Sistema RNP.

2. Fundamentação

A crescente adoção do paradigma de e-Ciência é caracterizada pela prática científica colaborativa em larga escala, sustentada por infraestrutura computacional distribuída e por organizações virtuais que extrapolam fronteiras institucionais (Jankowski, 2007; MacFarlane et al., 2003), impondo exigências rigorosas de governança de identidade, como acesso federado entre instituições, autenticação de usuários não acadêmicos, interoperabilidade entre os protocolos SAML e OIDC, e gerenciamento dinâmico de Organizações Virtuais [Mello et al. 2022]. Como resposta padronizada a esses requisitos, a GÉANT propôs a Arquitetura Blueprint AARC, amplamente adotada por infraestruturas científicas internacionais [Biancini et al. 2016]. No Brasil, esse cenário se reflete na estruturação, pela RNP, da Rede de e-Ciência nacional, apoiada no acesso federado da Comunidade Acadêmica Federada (CAFe), integrada ao eduGAIN.

3. Provas de Conceito

Para possibilitar a criação de Organizações Virtuais e garantir mais segurança e eficiência para a Rede de e-Ciência foram selecionadas duas plataformas: o CILogon [Basney 2019] da InCommon e uma solução baseada no MyAccessID [GÉANT 2022]. A plataformas foram submetidas a provas de conceitos com o objetivo de validar tecnicamente a viabilidade da adoção das soluções como provedores de autenticação federada, para este ambiente de e-Ciência.

3.1. CILogon

A motivação central desta PoC reside no fato de que o ecossistema de federação acadêmica brasileiro opera majoritariamente sobre SAML 2.0 via Shibboleth (CAFe/eduGAIN), enquanto as aplicações científicas modernas requerem nativamente OIDC/OAuth 2.0. A ausência de uma camada de tradução entre esses protocolos obriga cada provedor de serviço a implementar integrações isoladas, elevando custos de manutenção e riscos de segurança. Desta forma, torna-se necessário um *broker* de autenticação federada capaz de mediar SAML e OIDC, agregar identidades da CAFe, da eduGAIN e de provedores sociais, além de possibilitar o gerenciamento do ciclo de vida de identidades em OVs e o provisionamento de permissões nos serviços.

Para validar essa proposta, a PoC adotou uma implantação *self-hosted* do CILogon integrada à federação de experimentação CAFe Expresso. Como aplicação de estudo foi usado o GitLab, que utiliza o *framework* Omniauth para autenticação via SAML [GitLab 2026]. O SATOSA foi empregado como um proxy de tradução entre a interface OIDC do CILogon e a interface SAML do GitLab. O ciclo de vida de identidades (grupos, associações e funções) foi centralizado no COmanage Registry, com uma Organização Virtual dedicada e fluxo de autorregistro, sincronizado ao GitLab por meio de um conector em Python. Em termos de infraestrutura, a solução foi conteinerizada com Docker Compose e distribuída em dois *hosts* físicos, um dedicado ao CILogon (Serviço CILogon/Shibboleth SP e o *backend* OA4MP, que gerencia *tokens* e *endpoints* OIDC [NCSA 2025]) e outro hospedando GitLab, SATOSA e COmanage Registry, com PostgreSQL para persistência e Nginx como proxy reverso.

Sob o ponto de vista acadêmico, o trabalho contribui empiricamente para a literatura de IAM em e-Ciência ao demonstrar, em ambiente real, a viabilidade de um *broker* alinhado aos requisitos de [Mello et al. 2022] e à arquitetura AARC. Do ponto de vista prático, oferece um modelo replicável para centros de pesquisa brasileiros que precisem interoperar SAML com aplicações OIDC, preservando a soberania dos dados de identidade e abrindo caminho para expansão institucional e integração futura com a eduGAIN.

3.2. Solução Baseada no MyAccessID

Para a execução da PoC, o planejamento inicial previa a experimentação direta com o MyAccessID, solução voltada a cenários de autenticação e autorização para ambientes de pesquisa [GÉANT 2022]. Entretanto, diante da indisponibilidade de acesso ao código-fonte, a PoC adotou uma estratégia de implementação funcionalmente equivalente, utilizando componentes abertos capazes de reproduzir os principais papéis arquiteturais previstos na abordagem MyAccessID e na Arquitetura Blueprint AARC.

Para interoperar federações acadêmicas baseadas majoritariamente em SAML com aplicações modernas que consomem preferencialmente OpenID Connect (OIDC) e OAuth 2.0, a arquitetura foi estruturada em torno do Keycloak [Keycloak Project 2026], utilizado como núcleo de IAM, broker de identidade e servidor de autorização. O Keycloak foi responsável por centralizar o fluxo de autenticação, emitir tokens OIDC, manter sessões de usuário, mapear atributos e integrar fontes externas de identidade, incluindo LDAP. A mediação com a federação CAFe Expresso foi realizada por meio do SATOSA, empregado como proxy de tradução entre protocolos, uma vez que é projetado para intermediar fluxos envolvendo SAML2, OIDC e OAuth2 [IdentityPython 2025].

O fluxo principal validado na PoC inicia-se quando o usuário acessa uma aplicação protegida, que redireciona a requisição de autenticação para o Keycloak, responsável por encaminhar o usuário ao SATOSA. O SATOSA interage com o serviço de descoberta da CAFe Expresso, permitindo a seleção da instituição de origem e o redirecionamento ao provedor de identidade institucional. Após a autenticação no IdP, a resposta federada retorna ao SATOSA, que realiza a tradução necessária para que os atributos sejam consumidos pelo Keycloak. Por fim, o Keycloak associa a identidade ao usuário local, aplica os mapeamentos configurados e emite os tokens consumidos pela aplicação. Esse fluxo permitiu validar a autenticação federada com a CAFe Expresso sem exigir que cada aplicação implementasse diretamente a lógica SAML da federação.

Para apoiar a gestão de OVs, membros e grupos, a PoC utilizou o COmanage como componente de governança de identidades colaborativas. No ambiente implementado, o provisionamento via SCIM foi validado como funcional, permitindo propagar informações de usuários e grupos para a camada de IAM. De forma complementar, foi integrada uma base LDAP externa ao Keycloak, possibilitando a leitura de usuários, grupos e atributos Assim, a solução combinou COmanage/SCIM para governança de OVs e LDAP para interoperabilidade operacional com serviços consumidores.

A validação funcional da arquitetura foi realizada inicialmente com uma aplicação de teste baseada em React-SP, utilizada como Service Provider para observar o fluxo de autenticação, o retorno da sessão e os atributos recebidos. Em seguida, a solução foi integrada ao Open OnDemand, plataforma voltada ao acesso web a ambientes de supercomputação e aplicações HPC [Open OnDemand 2026]. Nesse cenário, o Open

OnDemand consumiu autenticação federada via Keycloak, permitindo que o usuário autenticado pela federação acessasse o dashboard da plataforma.

3.3. Conclusão

Como resultado das PoCs realizadas no ambiente do GidLab da RNP, foi possível observar um resultado positivo. Os testes conduzidos com CILogon confirmaram a estabilidade da pilha integrada, com *endpoints* OIDC funcionais, emissão e validação corretas de *tokens*, e fluxo de autenticação federada validado para CAFe Expresso (via SAML), Google e GitHub (via OIDC), incluindo mapeamento correto de atributos federados e processo de aprovação administrativa operacional. A solução baseada no MyAccessID, confirmou a viabilidade funcional da arquitetura proposta. As duas tecnologias apresentaram resultados promissores para aplicação no ambiente de e-Ciência. Entretanto, a ausência de código-fonte aberto do MyAccessID limitou a replicação dos testes e, consequentemente, uma avaliação mais abrangente da solução. Por outro lado, o CILogon foi avaliado em um ambiente real, permitindo uma análise mais próxima de sua utilização prática na e-Ciência. Como trabalho futuro, a eventual disponibilização do código-fonte do MyAccessID possibilitará a realização de novas análises e comparações entre as soluções.

Referências

Basney, J. e. a. (2019). CILogon: Enabling federated identity and access management for scientific collaborations. *Proceedings of Science, Sissa Medialab Srl, v. 351, 2019. ISSN 1824-8039. DOI: 10.22323/1.351.0031*.

Biancini, A., Florio, L., Haase, M., Hardt, M., Jankowski, M., Jensen, J., Kanellopoulos, C., Liampotis, N., Licehammer, S., Memon, S., van Dijk, N., Paetow, S., Prochazka, M., Sallé, M., Solagna, P., Stevanovic, U., and Vaghetti, D. (2016). AARC: First draft of the Blueprint Architecture for Authentication and Authorisation Infrastructures. *arXiv preprint arXiv:1611.07832*.

GitLab (2026). OmniAuth. Acesso em: 1 jun. 2026.

GÉANT (2022). Myaccessid identity and access management service. `https://wiki.geant.org/display/MyAccessID/`. Acesso em: 10 dez. 2025.

IdentityPython (2025). SATOSA: Proxy translating between different authentication protocols. `https://github.com/IdentityPython/SATOSA`. Acesso em: 6 jul. 2026.

Keycloak Project (2026). Keycloak: Open Source Identity and Access Management. `https://www.keycloak.org/`. Acesso em: 6 jul. 2026.

Mello, E., Chaves, S., Silva, C., Wangham, M., Brito, A., and Henriques, M. (2022). Autenticação e autorização: Antigas demandas, novos desafios e tecnologias emergentes. In *Minicursos Do XXII Simpósio Brasileiro de Segurança Da Informação e de Sistemas Computacionais*, pages 1–50. SBC.

NCSA (2025). OA4MP - OAuth for many people. Acesso em: 13 abr. 2026.

Open OnDemand (2026). Open OnDemand: Connecting Computing Power With Powerful Minds. `https://www.openondemand.org/`. Acesso em: 6 jul. 2026.

RNP (2024). Rede de e-ciência. `https://www.rnp.br/projetos/rede-de-e-ciencia`. Acesso em: 2 jul. 2026.