Avaliação Experimental de Estratégias de Agregação de Atributos em Federações Acadêmicas

Luiza Kuze Gomes[1], Maria Amanda de Freitas Morais[2], Estefânia Angelico Pianoski Arata[3], Fiterlinge Martins de Sousa[3], Reinaldo Cézar de Morais Gomes[3]

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

[2]Universidade Federal do Rio Grande do Norte (UFRN)

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

luiza.k12@aluno.ifsc.edu.br, amanda.morais.110@ufrn.edu.br,

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

Resumo. *Atributos são essenciais à autorização em ambientes federados. Este artigo avalia quatro modelos de obtenção de atributos em federações acadêmicas: Provedor de Identidade (IdP) como fonte e agregação pelo IdP, pelo Provedor de Serviço (SP) ou por proxy de identidade. Nos cenários de agregação, uma Autoridade de Atributos (AA) atua como fonte externa. Comparam-se desempenho na instância-base e escalabilidade federada.*

1. Introdução

Federações de identidade permitem que usuários de diferentes instituições acessem serviços compartilhados por meio de autenticação federada e relações de confiança. Em organizações virtuais colaborativas, o Provedor de Identidade (IdP) nem sempre mantém ou libera todos os atributos exigidos, tornando necessários mecanismos complementares de obtenção e agregação para autorização.

Este trabalho avalia experimentalmente quatro modelos de obtenção e agregação de atributos. O primeiro utiliza o IdP como fonte, enquanto os demais empregam uma Autoridade de Atributos (AA) externa, com agregação pelo IdP, pelo Provedor de Serviço (SP) ou por um proxy. A comparação considera custo de autorização, número de mensagens, tamanho das asserções SAML e escalabilidade da federação.

2. Trabalhos relacionados

A agregação de atributos em federações de identidade permite utilizar informações distribuídas entre diferentes autoridades no processo de autorização federada. [Chadwick et al. 2010] propuseram um modelo baseado em um *Linking Service* para integrar atributos de múltiplos IdPs, enquanto [Ferdous and Poet 2013] compararam modelos de agregação quanto à segurança, privacidade e interoperabilidade.

Posteriormente, [El Haddouti and El Kettani 2019] propuseram o *Account Linking Provider* (ALP) para agregar atributos de múltiplos IdPs em uma única sessão, enquanto [Priesnitz Filho et al. 2019] introduziram o *User Identification Strengthening* (UsIdS), com foco na privacidade. Mais recentemente, [Shemshi and Jakimovski 2025] exploraram um *Proxy AAI* para integrar diferentes estruturas de identidade, reforçando a relevância contemporânea das arquiteturas baseadas em proxy.

3. Fontes de atributos para autorização

Esta seção avalia quatro cenários da AARC-G006 (Figura 1): IdP como fonte e AA consultada por IdP, SP ou proxy [AARC Project 2017b]. A *AARC Blueprint Architecture* (BPA) 2019, atualizada pela BPA 2025, constitui a referência vigente; contudo, adota uma perspectiva arquitetural distinta, ao classificar onde informação, decisão e aplicação ocorrem [AARC Community 2019, AARC Community 2025]. Como a G006 classifica a fonte e o ponto de agregação, mantém-se adequada ao recorte. Com a decisão no SP, o proxy corresponde ao modelo *Centralised Policy Information Point*.

A BPA 2019 prevê o *Token Translation Service* (TTS), admitido pela AARC-G003, além de SP e proxy, como ponto de agregação [AARC Project 2017a]. O TTS não foi avaliado, pois todo o fluxo usa SAML, dispensando tradução de tokens.

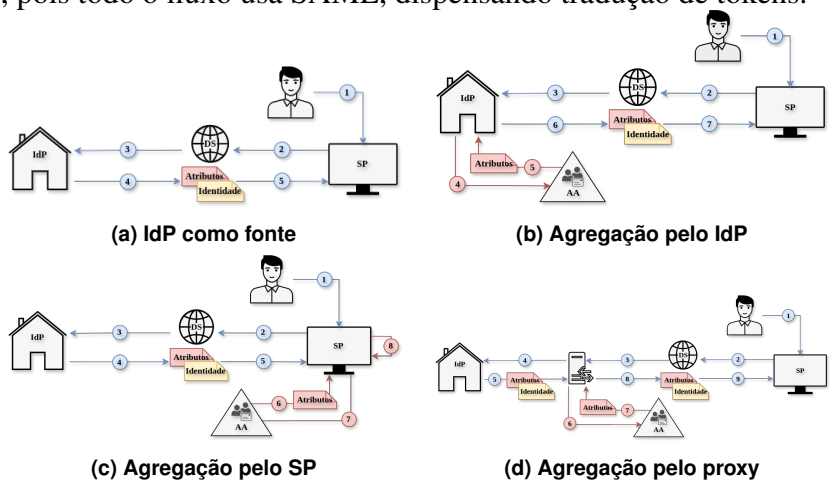

Figura 1. Modelos de fontes de atributos para autorização

3.1. IdP como fonte de atributos

Representado na Figura 1a, o fluxo ocorre em cinco etapas: (1) solicitação de acesso ao SP; (2) redirecionamento ao serviço de descoberta (DS); (3) seleção do IdP de origem e autenticação do usuário; (4) recuperação dos atributos institucionais e geração da asserção SAML pelo IdP; e (5) recebimento pelo SP para avaliação da política de acesso.

3.2. Agregação pelo IdP

Na Figura 1b, o fluxo mantém as etapas comuns (1)-(3) e segue com: (4) consulta do IdP à AA; (5) retorno ao IdP; (6) agregação aos atributos institucionais e geração da asserção SAML; e (7) recebimento pelo SP para avaliação da política de acesso.

3.3. Agregação pelo SP

Na Figura 1c, o fluxo mantém as etapas comuns (1)-(3) e segue com: (4) emissão da asserção SAML inicial; (5) envio ao SP; (6) consulta do SP à AA; (7) retorno dos atributos; e (8) agregação local para avaliação da política de acesso.

3.4. Agregação pelo proxy de identidade

Representado na Figura 1d, o fluxo ocorre em nove etapas: (1) solicitação de acesso ao SP; (2) redirecionamento ao DS; (3) envio da requisição ao proxy; (4) redirecionamento ao IdP e autenticação do usuário; (5) envio da asserção SAML ao proxy; (6) consulta do proxy à AA; (7) retorno dos atributos ao proxy; (8) agregação dos atributos e geração de resposta consolidada; e (9) recebimento pelo SP para avaliação da política de acesso.

4. Metodologia

Os cenários foram implementados em SAML [OASIS 2005], em um testbed compatível com a Comunidade Acadêmica Federada da RNP (CAFe), com IdP Shibboleth, SP em Python, AA simulada por API e SATOSA no caso com proxy [IdentityPython sd].

A avaliação teve duas fases: na primeira, o Locust [Locust 2026] avaliou o desempenho em uma instância-base com um IdP e um SP; na segunda, analisou-se a superfície de consulta à AA com o aumento das entidades. Implementação, código e configurações estão em: `https://github.com/luizakuze/atributos-wgid-2026`.

5. Resultados e Discussões

Na Fase 1, conforme a Tabela 1, o IdP como fonte teve o menor custo; IdP e SP, desempenho semelhante; e o proxy, o maior custo, pelo processamento e pela nova assinatura. A AA simulada por API não inclui latência externa nem controles de confiança, governança ou consentimento; logo, os tempos podem variar em produção. As mensagens crescem com os componentes, e a menor asserção do proxy decorre do *pysaml2*.

Tabela 1. Resultados experimentais das abordagens na instância-base

Critério	Fonte: IdP	Agregação: IdP	Agregação: SP	Agregação: proxy
Custo de autorização (ms)	39	65	64	150
Mensagens no fluxo	5	7	8	9
Asserção ao SP (kB)	12,8	13,5	12,8	10,9
Número de entidades	2	3	3	4
Consulta direta à AA	Não se aplica	IdP	SP	Proxy
Entidades sem consulta à AA	Não se aplica	SP, DS	IdP, DS	SP, IdP, DS

Na Fase 2, conforme a Tabela 2, avaliou-se a superfície de consulta à AA, excluindo o cenário sem AA externa. N indica as entidades consulentes e M, uma escala arbitrária. A superfície cresce com IdP ou SP e permanece constante com proxy.

Tabela 2. Superfície de consulta à AA com múltiplas entidades federadas

Entidades	Agregação: IdP	Agregação: SP	Agregação: proxy
$N = 1$	1	1	1
$N = 3$	3	3	1
$N = M$	M	M	1

6. Conclusão

A avaliação mostra que o IdP como fonte única de atributos apresenta menor complexidade e bom desempenho, mas não atende a cenários que dependem de atributos externos à instituição de origem, servindo como linha de base experimental.

Na Fase 1, as agregações pelo IdP e pelo SP apresentaram bom desempenho, porém a Fase 2 evidenciou limitações operacionais em escala. No primeiro caso, cada IdP precisa consultar a AA e coordenar políticas de liberação; no segundo, cada SP deve integrar-se à AA e compatibilizar identificadores.

O proxy apresentou o maior custo de autorização na Fase 1 devido ao overhead de processamento. Ainda assim, foi o único modelo que manteve constante a superfície de consulta à AA na Fase 2. Portanto, deve ser avaliado não apenas pelo custo individual, mas por seu papel arquitetural na integração escalável entre IdPs, SPs e fontes externas, em linha com estudos recentes sobre proxies em federações [Dalmazo et al. 2025].

Portanto, as abordagens pelo IdP ou pelo SP podem ser suficientes em ambientes pequenos, entretanto têm expansão limitada pela complexidade operacional. Em federações acadêmicas amplas, como a CAFe, com cerca de 2.500 serviços digitais [RNP 2026], o proxy se mostra mais adequado quando a autorização depende de atributos da colaboração, oferecendo melhor escalabilidade e maior controle arquitetural.

Referências

AARC Community (2019). AARC-G045: Blueprint Architecture 2019. `https://doi.org/10.5281/zenodo.3672784`. Acesso em: 5 ago. 2026.

AARC Community (2025). AARC-G080: Blueprint Architecture 2025. `https://aarc-community.org/guidelines/aarc-g080`. Acesso em: 5 ago. 2026.

AARC Project (2017a). AARC-G003: Attribute Aggregation. `https://aarc-community.org/guidelines/aarc-g003`. Acesso em: 5 ago. 2026.

AARC Project (2017b). AARC-G006: Best Practices for Managing Authorisation. `https://aarc-community.org/guidelines/aarc-g006`. Acesso em: 5 ago. 2026.

Chadwick, D. W., Inman, G., and Klingenstein, N. (2010). A conceptual model for attribute aggregation. *Future Generation Computer Systems*, 26(7):1043–1052.

Dalmazo, L., Farias, J., Ribeiro Filho, A., Gomes, L., Morais, M., Sousa, F., and Wangham, M. (2025). Testbed para proxies de gestão de identidades: Uma análise prática do Shibboleth, SimpleSAMLphp e SATOSA. In *Anais Estendidos do XXV Simpósio Brasileiro de Cibersegurança*, pages 93–101, Porto Alegre, RS, Brasil. SBC.

El Haddouti, S. and El Kettani, M. D. E.-C. (2019). A hybrid scheme for an interoperable identity federation system based on attribute aggregation method. *Computers*, 8(3):51.

Ferdous, M. S. and Poet, R. (2013). Analysing attribute aggregation models in federated identity management. In *Proceedings of the 6th International Conference on Security of Information and Networks*, pages 181–188.

IdentityPython (s.d.). *SATOSA*. Acesso em: 4 jul. 2026.

Locust (2026). Locust documentation. `https://docs.locust.io/`. Acesso em: 4 jul. 2026.

OASIS (2005). Assertions and protocols for SAML v2.0. `https://docs.oasis-open.org/security/saml/v2.0/`. Acesso em: 4 jul. 2026.

Priesnitz Filho, W., Ribeiro, C., and Zefferer, T. (2019). Privacy-preserving attribute aggregation in eID federations. *Future Generation Computer Systems*, 92:1–16.

RNP (2026). CAFe – comunidade acadêmica federada. `https://rnpmais.rnp.br/comunidade-academica-federada-cafe`. Acesso em: 7 jul. 2026.

Shemshi, V. and Jakimovski, B. (2025). Extended model for efficient federated identity management with dynamic levels of assurance across eIDAS, REFEDS, and Kantara frameworks for educational institutions. *Information*, 16(5):385.